Kerio Personal Firewall 4™

User's Guide

Kerio Technologies

© 1997-2004 Kerio Technologies. All rights reserved.

Printing Date: February 02, 2004

This guide provides detailed description on the *Kerio Personal Firewall*, version *4.0.11*.
All additional modifications and updates reserved.

For current product version, check `http://www.kerio.com/kpf`.

Contents

1 Introduction 5
- 1.1 Kerio Personal Firewall 4.0 5
- 1.2 Limited Free Edition 7
- 1.3 System Requirements 8
- 1.4 Conflicting Software 8
- 1.5 Installation, Upgrade and Uninstallation 9
- 1.6 Update Checks 10
- 1.7 Initial Configuration 11

2 Firewall Components and Basic Control Features 13
- 2.1 Kerio Personal Firewall Components 13
- 2.2 Icon on the Systray 14
- 2.3 Registration 16

3 Firewall Behavior and Interaction with Users 21
- 3.1 Firewall Behavior 21
- 3.2 Connection Alert (unknown traffic detection) 21
- 3.3 Starting/Replacing/Launching other application Dialog 25
- 3.4 Alert Dialog Window (alerts on events) 28

4 Firewall Configuration 31
- 4.1 Configuration Dialog 31
- 4.2 Remote Administration 34
- 4.3 Preferences 37

5 Network Security 43
- 5.1 How the Firewall Policy is Applied 43
- 5.2 Rules for Applications 44
- 5.3 Network Security Predefined Rules 47
- 5.4 Trusted Area Definition 49
- 5.5 Advanced Packet Filter 51

6 System Security 63
- 6.1 Application Rules 63
- 6.2 General Rules 65

7 Internal Firewall Rules 67
7.1 Internal Network Traffic Rules 67
7.2 System Security Rules 69
7.3 Rules for AVG components 71

8 Intrusions Detection System 73
8.1 IDS Settings 73

9 Web Content Filtering 77
9.1 The *Ad blocking* tab 77
9.2 The *Privacy* tab 81
9.3 The *Exceptional sites* tab (exceptions for individual servers) 82

10 Status Information and Logs 85
10.1 Connections and Open Ports Overview 85
10.2 Statistics 86

11 Logs 89
11.1 Logs Viewing 89
11.2 Logs Context Menu 90
11.3 Log Options 91
11.4 Network Log 92
11.5 System Log 93
11.6 Intrusions Log 94
11.7 Web Log 95
11.8 Debug, Error, Warning Logs 96

12 Glossary 99

Chapter 1

Introduction

1.1 Kerio Personal Firewall 4.0

Kerio Personal Firewall is a software application protecting personal computers from external intrusions (typically from the Internet), viruses and data leak. Security is provided especially by the following four components:

Network Security This module controls all network (TCP/IP) traffic of the computer on which *Kerio Personal Firewall* is installed. Two types of rules can be defined for network communication:

- application rules — it is possible to permit/deny network communication for individual applications or set that *Kerio Personal Firewall* asks user.
- packet filter rules — advanced packet rules for network traffic can be defined (specification of IP addresses, protocols, ports, etc.). These rules can be applied either on individual applications or generally (on any application).

Kerio Personal Firewall includes set of predefined network security rules (i.e. for DNS, DHCP, etc.). These rules are separated from user-defined rules and they can be enabled or disabled.

Whenever *Kerio Personal Firewall* detects traffic which does not meet any rule, user will be asked to permit or deny the communication. Optionally, a corresponding application or packet filter rule can be created automatically upon this decision.

System Security The *System Security* module controls running applications in the operating system.The following event types are controlled:

- running applications
- replacements of the application's executable file since the last startup (application replacement)
- running another application by the particular application

Like in case of network traffic, rules for individual applications can be defined. These rules either permit or deny the event, eventually they ask user. If s communication

does not meet any rule, *Kerio Personal Firewall* automatically asks user to permit or deny running the application.

Note: Kerio Personal Firewall 4.0 (unlike older versions) controls running of all applications, regardless of the fact whether they participate in network communication or not. When infected, the firewall is more reliable than any antivirus (if the virus is new and it is not included in a particular virus database, antivirus is not able to detect it — *Kerio Personal Firewall* detects replacement of the executable file and warns user).

Intrusion detection The *Intrusion Detection System* (IDS) can distinguish, block and log known intrusion types. For this purpose *Kerio Personal Firewall* uses database of known intrusions. This database is updated regularly (updated database is included in new product versions).

Web content filtering This module enables the following features:

- blocking of ads (according to URI/URL rules), scripts and other Web items
- blocking of pop-up windows
- blocking of scripts (*JavaScript*, *VB Script*)
- protection from undesirable cookies storage and outflow of private data from Web application forms.

Exceptions (specific settings) can be defined for trustful servers and for cases when filtering might cause malfunctions.

The following functions and features are also provided by *Kerio Personal Firewall*:

Stop all traffic Use this button (or the option in the menu) to stop all traffic on the computer on which *Kerio Personal Firewall* is installed (so called network lock). This function may be very helpful especially when an undesirable or a queer network activity is detected — traffic can be restored when appropriate actions are taken.

Logging Each firewall module creates an independent log which is stored into a text file. Logs can be viewed in *Kerio Personal Firewall* configuration dialog. Optionally, logs can be stored on a *Syslog* server.

Connections overview and statistics The overview provides information on established connections and ports opened by individual applications. Information on current speed and size of transmitted data in both directions is also provided for active connections. The overview is refresh automatically in predefined time intervals.

Statistics inform user on number of objects blocked by the Web content filter and number of detected intrusions per a certain time period.

Automatic update *Kerio Personal Firewall* performs regular checks for new versions. Whenever a new version is detected, download and installation is offered. Checks for new versions can be also performed by hand.

Warning: None of the versions of the *Kerio Personal Firewall 4* can be used on Windows Server operating systems, such as Windows NT Server, Windows 2000 Server and Windows Server 2003.

1.2 Limited Free Edition

Two editions of *Kerio Personal Firewall* are available: full (paid) and free (free of charge, but limited).

The same installation package is used for both version. After installation the product behaves as a 30-days trial version (full version limited by time). If the product is not registered by the expiration date, it becomes free and limited. The product becomes a full version after license purchase and product registration (for detailed information refer to chapter 2.3).

Free (unregistered) editions are limited by the following restrictions:

- It is available for personal and/or noncommercial use only.
- Web content filtering, including its logs and statistics, is not available (see chapter 9).
- It cannot be used at Internet Gateways (refer to chapter 4.3)
- Logs cannot be sent to *Syslog* server (details in chapter11.3).
- Configuration cannot be protected by a password and it is not possible to access and administer the firewall remotely.

Technical Support

Only e-mail technical support is provided for issues concerning *Kerio Personal Firewall*. Owners of multi-licences (licences for more than one user/computer) can also contact our technical support by telephone. Go to `http://www.kerio.com/` to find detailed contact information.

1.3 System Requirements

The following hardware and software equipment is required for *Kerio Personal Firewall* installation:

- Windows 98 / Me / NT 4.0 Workstation / 2000 Professional / XP Home / XP Professional operating systems
- CPU Intel Pentium or 100% compatible
- 64 MB RAM
- 8 MB of free disc space (for installation only, 10 MB recommended for log files)
- minimal screen resolution 800x600 pixels

1.4 Conflicting Software

Kerio Personal Firewall might conflict with certain application types which are based on identical or similar technologies as *Kerio Personal Firewall*. Kerio Technologies does not guarantee correct functioning of *Kerio Personal Firewall* nor your operating system if any of the following software applications are installed on the same operating system:

Personal firewalls Personal firewalls (i.e. *Internet Connection Firewall* — a Windows XP component, *Zone Alarm*, *Sygate Personal Firewall*, *Norton Personal Firewall*, etc.) provide similar functions as *Kerio Personal Firewall*. Do not combine *Kerio Personal Firewall* with other firewalls.

Network firewalls Network firewalls (i.e. *Kerio WinRoute Firewall*, *Kerio WinRoute Pro*, *Kerio WinRoute Lite*, *Microsoft ISA Server*, *CheckPoint Firewall-1*, *WinProxy* by Ositis, *Sygate Office Network*, *Sygate Home Network*, etc.) also protects the computer on which it is installed, it is therefore not necessary to use a personal firewall on such computer.

Note: To create an elementary network firewall, *Kerio Personal Firewall* can be combined with a router, with a router which performs translation of IP addresses (NAT) or with a proxy server — i.e. *Internet Connection Sharing* (included in newer Windows operating systems). For detailed information refer to chapter 4.3.

1.5 Installation, Upgrade and Uninstallation

Installation

Run the installation program (i.e. `kerio-pf-4.0.0-en-win.exe`). A path which will be used for the *Kerio Personal Firewall* installation can be specified during the installation process

(`C:\Program Files\Kerio\Personal Firewall 4` by default).

Restart is necessary after a successful installation, so that the *Kerio Personal Firewall* low-level driver can be enabled.

Warning: If you intend to use *Kerio Personal Firewall* with the *AVG* antivirus, *AVG* must be installed before the *Kerio Personal Firewall* installation is initiated. If *Kerio Personal Firewall* detects the *AVG* antivirus when the firewall is started first time, corresponding rules will be set for the antivirus (refer to chapter 7.3).

Notes:

1. Updating of your *Windows Installer* might be required under Windows 98, Me, NT 4.0, if it has not been updated yet (i.e. during installation of another application). The update requires approximately 1.8 MB. The *Windows Installer* update file must be downloaded and installed to enable *Kerio Personal Firewall* installation!

2. Memory dump which can be used when the system crashes is created in Windows NT operating systems. User can send it to *Kerio Technologies* — analysis of the dump may help find and remove bugs and errors which caused the crash.

   Check an option (see chapter 4.3) to set memory dump generating in the operating system.

Upgrade

Installation of a new version (upgrade) is performed in the same method as a new installation described above. It is not necessary to stop running components of the application since they will be automatically stopped and closed by the installation program.

Note: Kerio Personal Firewall includes a built-in system for automatic checks and downloads of updates (for details see chapter 1.6).

Uninstallation

Kerio Personal Firewall can be uninstalled using the *Add / Remove programs* option in the *Control Panel*. Files which have been created after the installation (configuration

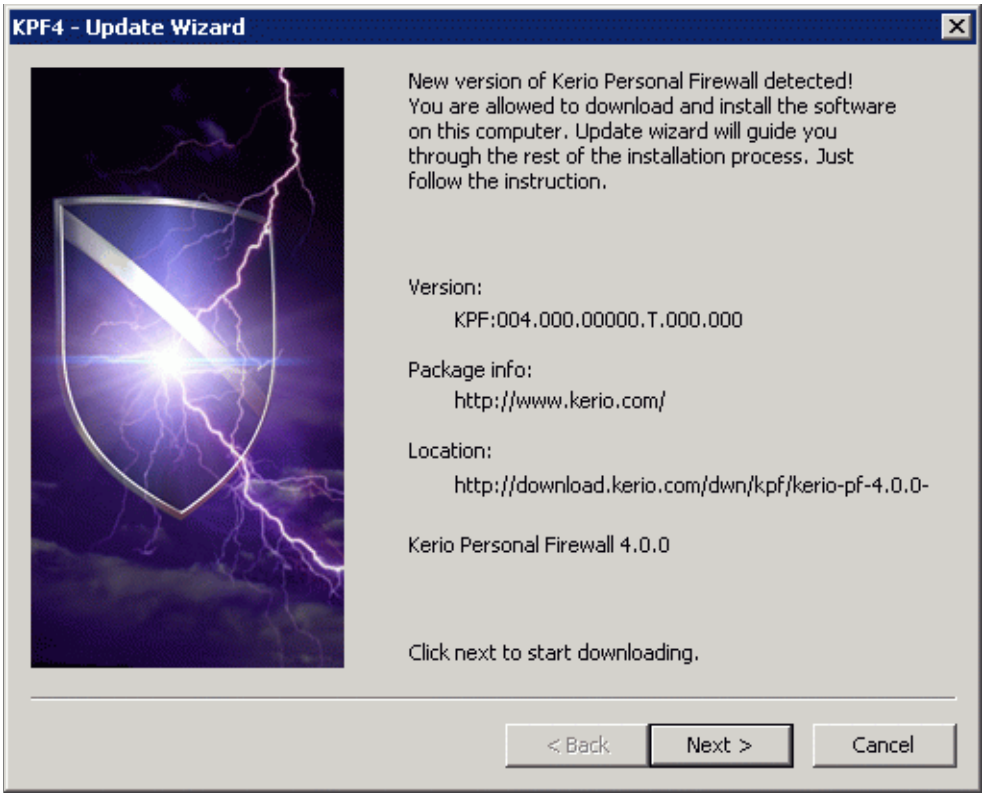
files, logs, etc.) will not be removed. These files can be either removed by hand or kept for the next installation.

1.6 Update Checks

Kerio Personal Firewall provides automatic checks for new versions. These versions, if detected, can be downloaded. Automatic checks are provided after each start of *Personal Firewall Engine* and then every 24 hours.

Checks for new versions can be also run by hand using the *Check now* button in the *Overview / Preferences* section of the *Kerio Personal Firewall* configuration dialog (for details see chapter 4.3).

If you already have the latest version of *Kerio Personal Firewall*, the connection with the server is closed and the next check is scheduled. If a new version is detected, information on this version and its download is provided.



Click on the *Next* button to start download of the new version and to run the installation program. *Kerio Personal Firewall* always checks signature of a downloaded file — this feature ensures that any downloaded file will be original (it is not attacked by a virus, dammaged, etc.).

The system must be restarted after a new version is installed.

The download or the installation process can be stopped by the *Cancel* button. If the process is canceled, the update will not be offered again automatically, however, it can be run by hand whenever needed. When a new version is found, *Kerio Personal Firewall* will open the update dialog automatically.

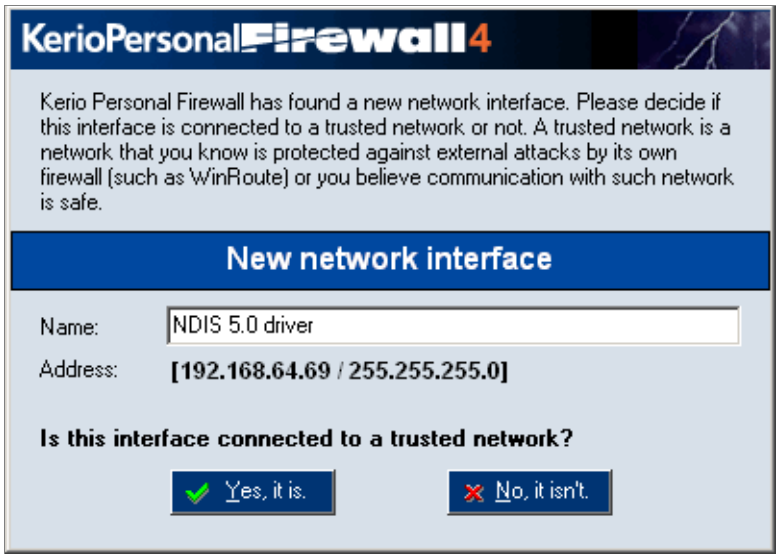
For detailed information on the *Kerio Personal Firewall* installation refer to chapter 1.5.

Note: Kerio Personal Firewall follows special internal rules which always allow access to the server where the product can be updated and registered. Therefore, the automatic update checks cannot be blocked by inappropriate firewall settings.

1.7 Initial Configuration

During the first start after the installation, *Kerio Personal Firewall* detects active network interfaces of the computer on which it is running. A dialog asking whether the interface is connected to a trusted network is opened for each detected interface.

Trusted network is a network which is considered secure. It is typically a local network protected from external intrusions and viruses by a network firewall. *Kerio Personal Firewall* enables definition of various rules for trusted networks and for the Internet (for details go to chapter 5.4).



This dialog provides a *Name* of a corresponding network interface as well as its IP address and network mask (mask of the network to which the interface is connected) which are represented by the *Address* item.

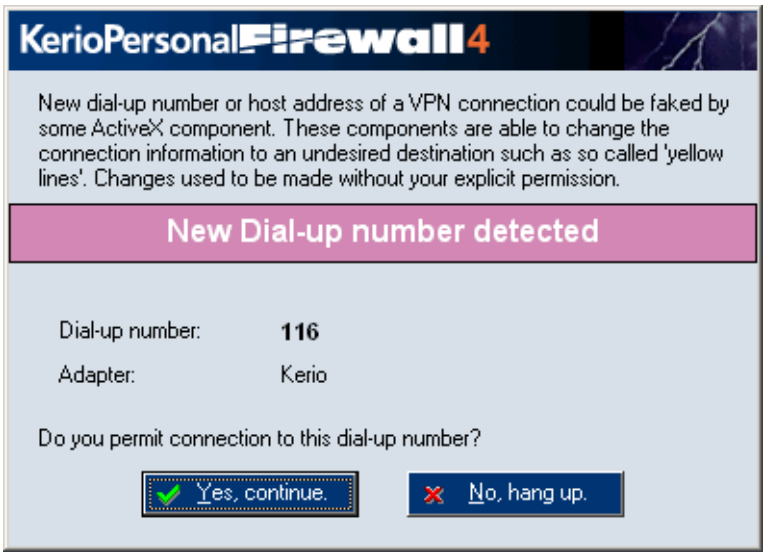
Use the *Yes, it is* button to acknowledge the subnet to which the particular interface is connected as trusted and to add it to the group of trusted IP addresses. Use the *No, it isn't* button to consider the particular subnet as a part of the Internet.

Notes:

1. Configuration of trusted IP addresses can be modified anytime (for detailed information refer to chapter 5.4).

2. Anytime a new interface is added or enabled or the interface is connected to another subnet, *Kerio Personal Firewall* detects it automatically and opens the dialog described above.

3. In case of dial-up connection a corresponding telephone number is checked. If *Kerio Personal Firewall* detects change of telephone number, user is asked whether the change will be accepted. This protects user from undesirable change of dial-up connection parameters (i.e. by an ActiveX object on a Web page).



New number is displayed as the *Dial-up number* item (telephone number which is set for a corresponding dial-up connection at the moment).

Click on the *Yes, continue* button. *Kerio Personal Firewall* will accept the new number and allow connection to the line. Use the *No, hang up* option to reject the replacement — the line will be hung-up.

Chapter 2

Firewall Components and Basic Control Features

2.1 Kerio Personal Firewall Components

Low-level driver *Kerio Personal Firewall's* low-level driver is implemented into the core of an operating system during its startup. It is located between drivers of network interfaces and the TCP/IP subsystem. Therefore it is able to detect and test all IP traffic.

The low-level driver is stored in Windows system directory:

- as the `fwdrv.sys` file typically in the `C:\WINNT\system32\drivers` directory under the Windows NT and Windows 2000 operating systems
- as the `fwdrv.sys` file typically in the `C:\WINDOWS\system32\drivers` directory under the Windows XP operating system
- as the `fwdrv.vxd` file typically in the `C:\WINDOWS\system` directory under the Windows 98 and Windows Me operating systems

Personal Firewall Engine Core of the *Kerio Personal Firewall*. It is running as a service or in the background (Windows 98 and Me).

The *Personal Firewall Engine* service is stored in the `kpf4ss.exe` file in the installation directory of *Kerio Personal Firewall*. *Personal Firewall Engine* contains so called driver interface library which is stored in the `kfe.dll` file.

Personal Firewall GUI User interface of *Kerio Personal Firewall* (*GUI — Graphical User Interface*).

The *Personal Firewall GUI* component is automatically started by the *Personal Firewall Engine* service (when it is started or everytime it detects that the user interface is not running). When it is running, the *Personal Firewall GUI* is represented by a shield icon on the System Tray.

Right-click on the icon on the System Tray to open *Kerio Personal Firewall* configuration dialog or to use another option from the menu (stopping network traffic, disabling firewall, etc.). For details refer to chapter 2.2.

The *Personal Firewall GUI* is represented by the `kpf4gui.exe` file which can be found in the *Kerio Personal Firewall* installation directory.

Keyboard hooker This module enables to disable pop-up blocking temporarily using a hotkey (refer to chapter 9.1). It is represented by the `gkh.dll` file.

Crashdump sender This tool sends crashdump to the *Kerio Technologies* when *Kerio Personal Firewall* breaks down. It is represented by the `assist.exe` file.

Support for Fast User Switching

Kerio Personal Firewall supports *Fast User Switching* in Windows XP.

Multiple *Personal Firewall GUI* instances can be open at any moment. In such cases *Personal Firewall Engine* communicates with the session which belongs to the currently active user.

After startup of the operating system and the *Personal Firewall Engine* service, the first instance is executed that runs under the system account (or the account under which the *Personal Firewall Engine* service is executed). Upon user login a new instance of the *Personal Firewall GUI* is executed, running with the privileges of the logged user. This instance is active until the user logs off (the instance is terminated) or the user-switch function is used (the instance is only deactivated).

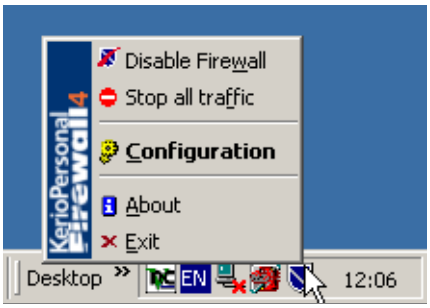
2.2 Icon on the Systray

Kerio Personal Firewall's shield-shaped icon is displayed on the System Tray whenever the*Personal Firewall GUI* component is running. This component is started automatically by the *Personal Firewall Engine*.

The *Kerio Personal Firewall* icon also represents network activity of the computer on which the firewall is installed. Network traffic is represented by little colored bars at the bottom of the icon:

- green bar — outgoing traffic
- red bar — incoming traffic

Double-click on the icon with the left mouse button to open the *Kerio Personal Firewall* configuration dialog (for details on firewall configuration see chapter 4). Right-click on the icon to open a menu providing the following options:



Disable Firewall This option disables the firewall. Use this option to disable all *Kerio Personal Firewall* modules (network communication filtering, monitoring of launched applications,intrusions detection and Web content filtering).

This option disables the firewall for certain necessary periods, such as during tests or debugging (i.e. network connection failures). We do not recommend you to use the *Disable Firewall* for long — the firewall would not function and your computer would not be protected.

When *Kerio Personal Firewall* is disabled, the icon striked-through.

This option disables the firewall and switches into the *Enable Firewall* mode. The *Enable Firewall* option can then be used for the firewall recovery.

Stop all traffic This option blocks all network traffic (network lock).

If this option is enabled, the “do not enter” sign is diplayed on the *Kerio Personal Firewall* shield icon.

This option in the menu changes to the *Enable traffic* option — it can be used to refresh the traffic applying the current firewall settings and rules.

HINT: In case that a network traffic that should have been denied was permitted by mistake. Use the *Stop all traffic* option to stop all active connections and to prohibit

its recovery. If a traffic rule has been created (using the *Create a rule for this communication* option), it can be removed (see chapters 5.2 and 5.5) and the traffic can be enabled again.

Note: Anytime the *Personal Firewall Engine* service is started up, the *Disable Firewall* and *Stop all traffic* options are set to default modes. For security reasons it is not recommended to leave the firewall disabled after the system startup. Stapping all traffic might cause problems for example during user login.

Configuration Use this option to open the *Kerio Personal Firewall* configuration dialog. Go to the chapter 4 to get more details on the firewall configuration.

Register This option runs registration wizard (for details refer to chapter 2.3). If *Kerio Personal Firewall* has been already registered, the option will not be available in the menu.

About The "About" window provides information on versions of individual *Kerio Personal Firewall* components as well as on expiration dates of limited versions and on the particular license.

Exit Use this option to stop the *Personal Firewall Engine* service and to close the *Personal Firewall GUI* (all open windows and application dialogs will be closed and the icon on the Systray will be hidden). If at least one dialog is open at the moment (i.e. *Connection Alert*), the option must be confirmed by user first.

Warning: If *Kerio Personal Firewall* is stopped, your computer is not protected anymore! *Kerio Personal Firewall* can be reactivated by starting the service in *Administrative Tools / Services*.

If access to the firewall administration requires a password and the user is authenticated, the *Logout* item is also available in the context menu. For detailed information refer to chapter 4.2.

2.3 Registration

After purchase of a product license, *Kerio Personal Firewall* must be registered. Features which are not available in the freeware version are activated by the registration (see chapter 1.2). Full technical support is also provided for registered products.

Note: Kerio Personal Firewall is free of charge for personal and noncommercial use. In such cases registration is irrelevant. However, 30 days after the installation *Kerio Personal Firewall* starts to behave as a limited version — see chapter 1.2

Kerio Personal Firewall can be registered by two ways:

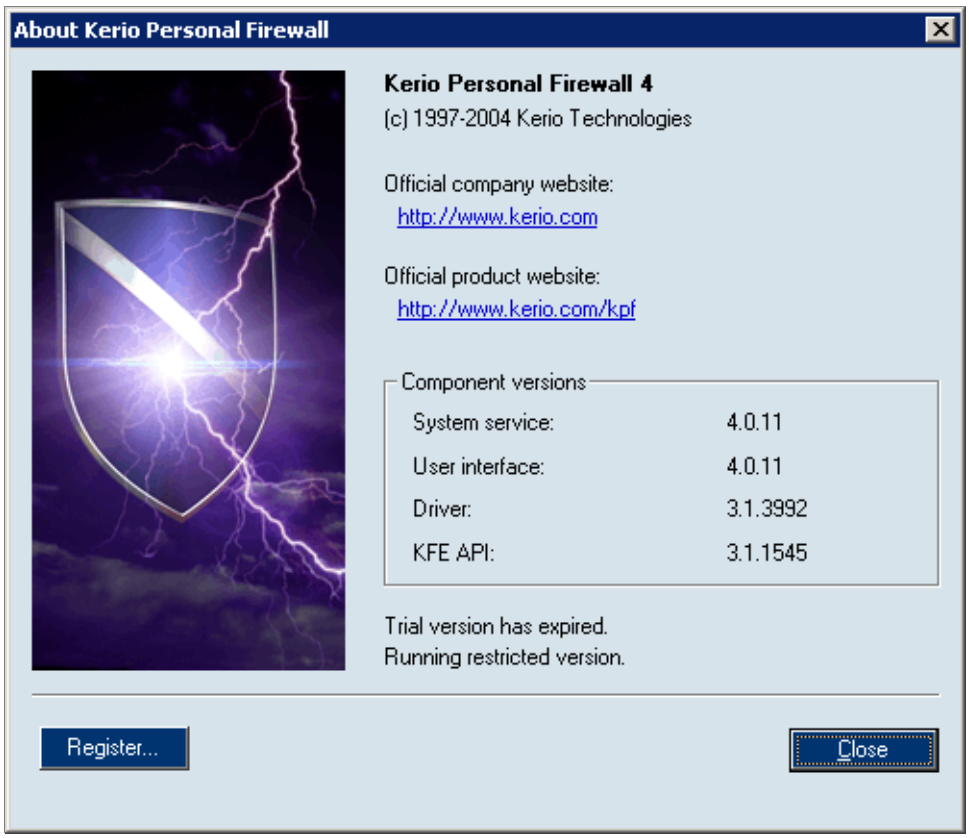
1. At the *Kerio Technologies* website (`http://www.kerio.com/`, the *eShop / Licence registration* section). Use a corresponding form to specify your registration number which you obtained after the product purchase. Then, a license key will be created (the `license.key` file). Download this key and save it to the `license` subdirectory in the directory where *Kerio Personal Firewall* is installed

   (typically `C:\Program Files\Kerio\Personal Firewall 4\license`).

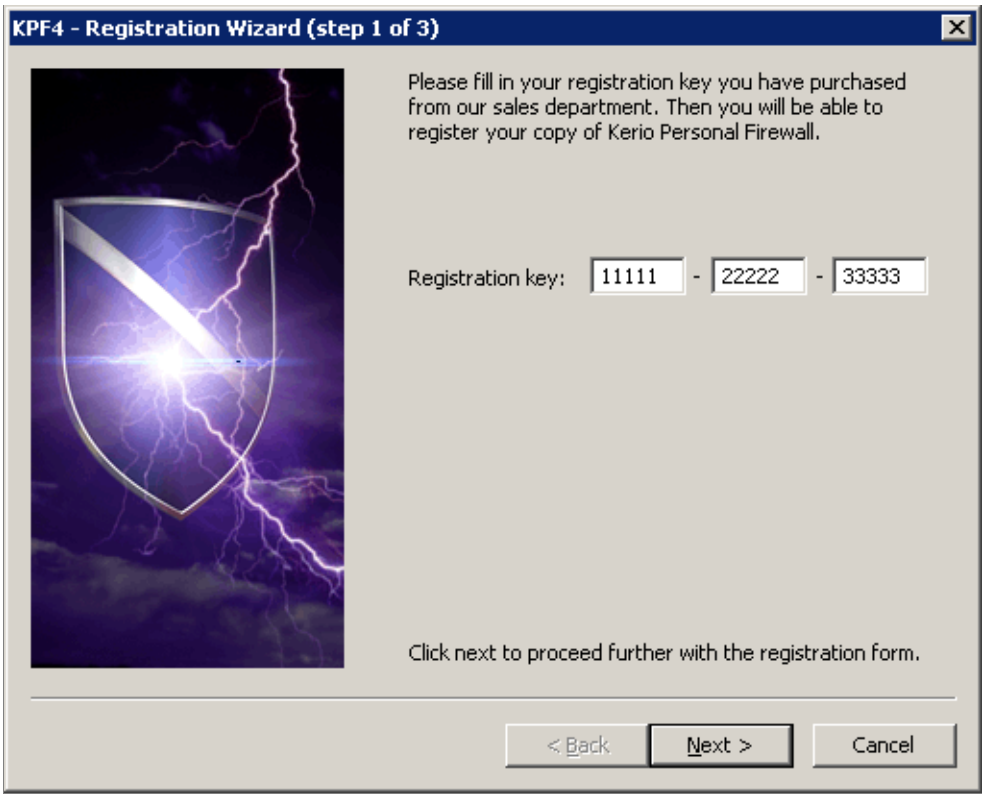
   Next time the *Personal Firewall Engine* service is run, the product will behave as a full version.

   HINT: This way of registration can be used when the computer with the *Kerio Personal Firewall* cannot be connected to the *Kerio Technologies* server (i.e. when traffic is blocked by a network firewall).

2. Using the *Registration Wizard*. The wizard can be run through the *Register* option in the context menu on the Systray (see chapter 2.2), through the *Register...* button in the configuration dialog or in the *About Kerio Personal Firewall* dialog (this dialog can be entered using the *About* option).



First, insert your registration number (*Registration Key*) which you acquire by the purchase of the product.



In the second dialog, specify data of a company or a person to which the registration is bound.

The *Company/Name* (name of the company or person), the *Country* and the *E-mail* (email address) entries are obligatory. The other items are optional.

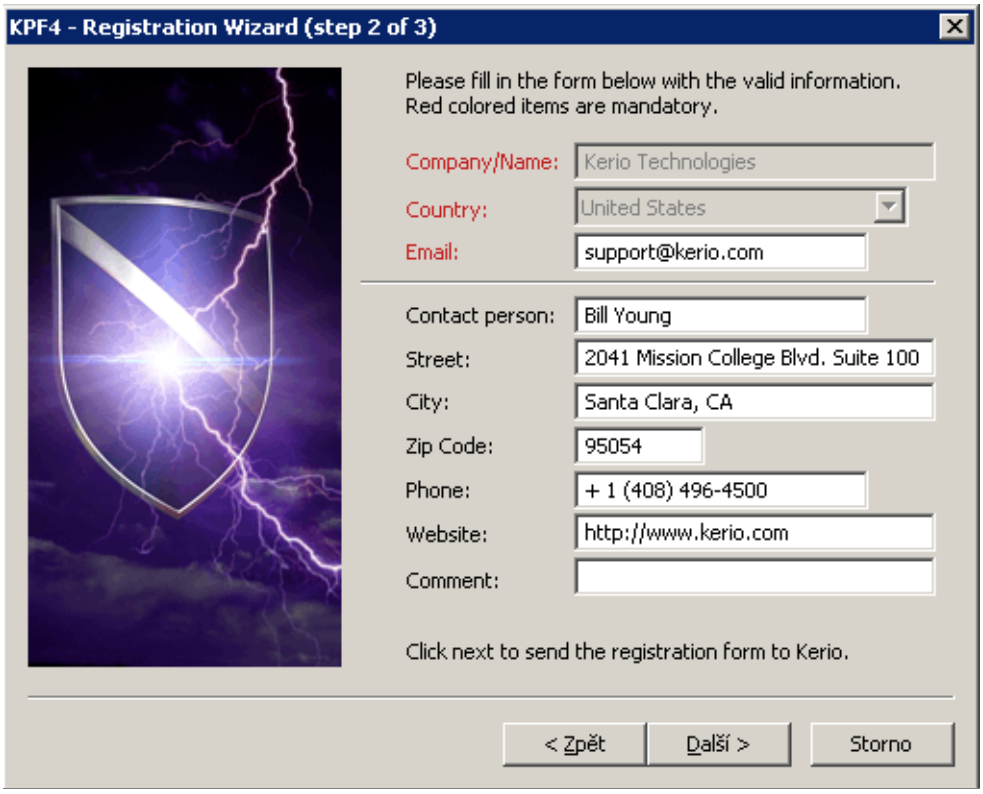
Click on the *Next* button to connect to the registration server. Inserted data will be verified and the license key will be downloaded automatically (digital certification).

In the third step information on the registration process will be shown.

In case of time limited license, *License expiration* date and *Subscription expiration* date (date by which free product updates expire) will be displayed .

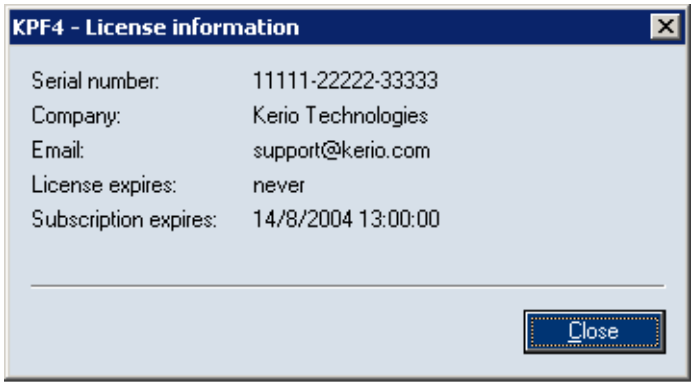
Click on the *Finish* button to close the wizard.

When the product is registered successfully, *Personal Firewall GUI* is restarted automatically. This will enable all functions which are not available in the unregistered version.



Viewing License Information

Next time the *About Kerio Personal Firewall* dialog is opened, the *License info* button will replace the *Register* button. Use the *License info* button to open open a window providing license information:



- *Serial number* — serial number of the product
- *Company* — company by which the product is registered

- *Email* — contact email address
- *License expires* — date of license expiration (*never* — the license is not limited by time)
- *Subscription expires* — date of subscription expiration (expiration of free product updates)

Chapter 3

Firewall Behavior and Interaction with Users

3.1 Firewall Behavior

Data transmission within the Internet is performed through TCP/IP protocols. These protocols are also used for most of traffic within local networks. The essential protocol is IP (Internet Protocol). Packets of this protocol carry the rest of information (they incapsulate other protocols). *Kerio Personal Firewall* controls all IP packets — this implies that it is able to catch them, get essential information and then either let them into the system or filter them out. Logs on all events, detected intrusions etc. are provided as well.

Kerio Personal Firewall is based on so called stateful inspection. This means that a log is created for each permitted connection and the firewall blocks all packets which do not belong to this connection.

Kerio Personal Firewall works in so called self-taught mode. Anytime unknown network traffic is detected, a dialog will be displayed through which the particular traffic can be permitted or denied, either for the single situation or for any further connections (permanently). If traffic is permitted/denied permanently, a corresponding rule is created automatically and users will not be asked about the particular traffic anymore. For details refer to chapters 3.2 and 5.5.

Filtering rules can be used by users/administrators for further traffic filtering. Only packets meeting required criteria are let through the firewall.

The same method is applied when an application is first launched (for details see chapter 6.1).

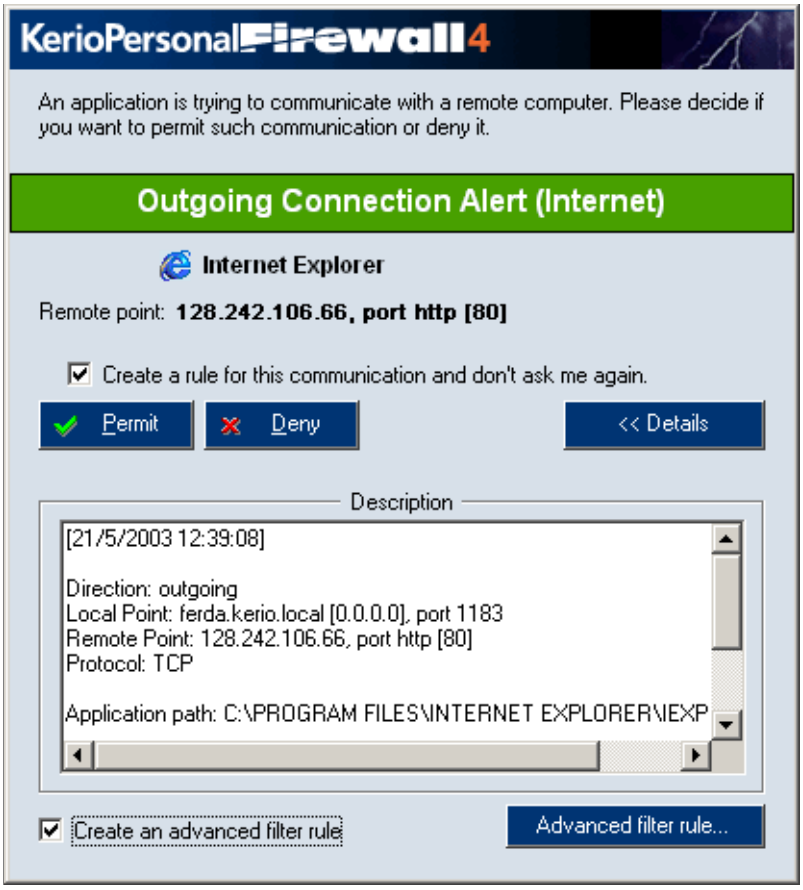
3.2 Connection Alert (unknown traffic detection)

The *Connection Alert* dialog (asks user whether the connection will be permitted or denied) informs users when *Kerio Personal Firewall* detects an unknown traffic. In this dialog, the user/administrator decides whether the traffic will be permitted or denied and if a corresponding rule is to be created.

Note: The way how *Kerio Personal Firewall* will behave when a network connection is detected are defined by parameters in the *Network Security* section (see chapters 5.2

and 5.3). The *Connection Alert* dialog is opened if no corresponding rule is found or the rule asks user explicitly.

This dialog is displayed "Always on Top". Whenever multiple concurrent events (multiple connection attempts or an attempt to open multiple applications at one moment — see chapter 3.3) are detected, these events are queued — the dialogs are opened in turn when a current dialog is answered.



The *Alert* dialog provides the following information and options:

Traffic direction and zone The colored stripe informs users of traffic direction (incoming or outgoing) and the location which a remote point belongs to (trusted IP addresses or the Internet).

The color of the stripe and the first part of the text represent the direction of the connection:

- *Outgoing connection alert* — outgoing connection (connection from a local to a remote point).

  Outgoing connections are represented by a green stripe.

- *Incoming connection alert* — incoming connection (connection from a remote to a local point).

  Incoming connection is represented by a red stripe.

The location where the IP address of a particular remote point belongs to is displayed in parenthesis:

- *Trusted area* — group of trusted IP addresses (for details see chapter 5.4)
- *Internet* — any IP address which is not included in the *Trusted area*

Local application and Remote point Basic information on an connection can be found below the colored stripe:

- application icon and its description used by the local computer. If a description is not available, the name of a corresponding executable file is displayed. If an application has no icon, a default system icon for executables will be used.
- remote point DNS name and its IP address (in brackets).

  Note: DNS names are identified through DNS queries. If a corresponding DNS name is found, it substitutes the IP address. Translation of IP addresses to DNS names can be enabled/disabled globally, for example in the *Overview / Connections* context dialog (see chapter 10.1)

- remote point (in case of standard services, the name of the service is displayed in addition to the port number)

Place the mouse pointer over the application name (description) to view a tooltip informing on a full path to the application's executable file.

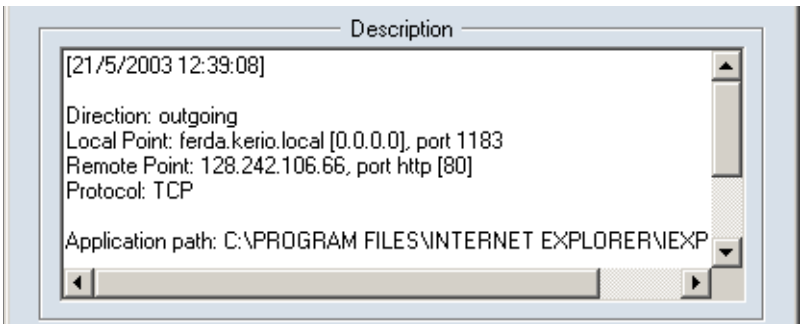
Actions The three following actions can be taken within the dialog:

- Use the *Permit* button to allow the connection.
- Use the *Deny* button to block the traffic.
- Check the *Create a rule for this communication and don't ask me again* option to create a rule for the particular communication. The system will remember the action that will be taken with this connection and create a corresponding rule. Later when identical connection is detected, *Kerio Personal Firewall* will automatically take an action meeting this rule (*Permit* or *Deny*).

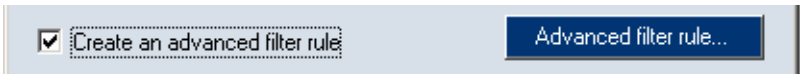
  Note: Created rules can be edited or removed using the *Kerio Personal Firewall Administration* dialog in the *Applications* tab of the *Network Security* section. For details refer to chapter 5.2.
- Use the *Details* button to view detailed information on the connection and on a corresponding local application. Click on this button again to hide this information.

Click on the *Details* button to view the following information:

Detailed information on the connection and local application In the description box there are details about the connection (direction, protocol, local/remote endpoint address and port number) and communicating application (name of executable file including the full file path, description of the application, date of file creation, the date of last change and the date which the file was last opened)



Create an advanced rule



Check the *Create an advanced filter rule* option to create (instead of a standard application rule —see chapter 5.2) an additional advanced rule which can be used to set details such as parameters for communication (IP addresses, ports, etc.), a local application, time validity, etc.

Click on the *Advanced filter rule...* button to open a dialog for an advanced definition of a packet filter rule. In this dialog a selected rule can be easily customized. Advanced rules can be edited or removed anytime using the *Packet Filter* button in the *Kerio Personal Firewall Administration* dialog in the *Applications* tab of the *Network Security* section.

Detailed information on advanced traffic rules are provided in chapter 5.5.

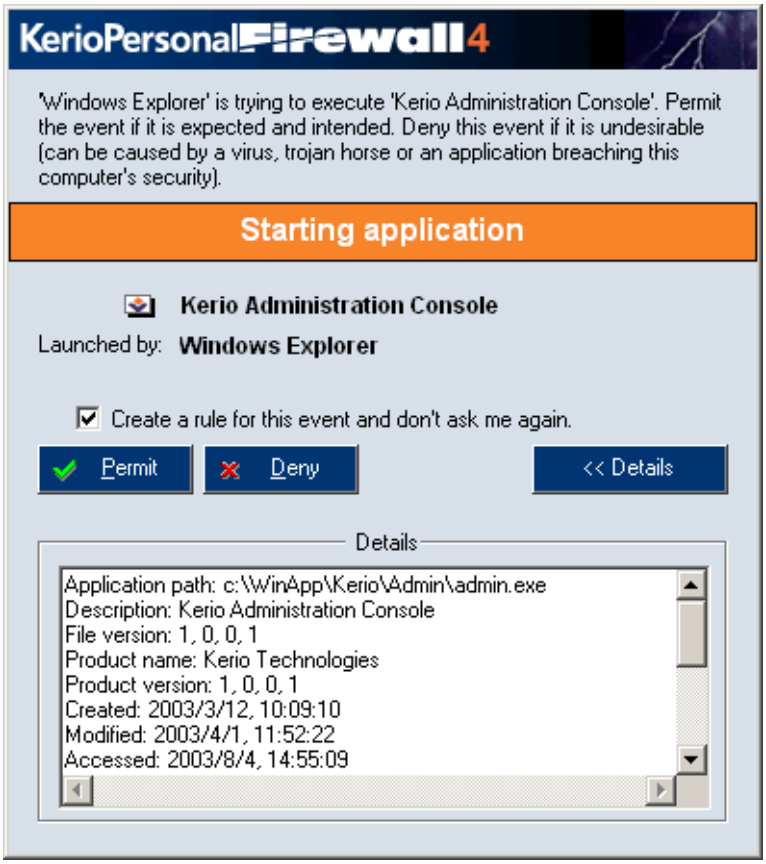
Note: The specific traffic in question is paused while the *Connection Alert* dialog is opened (the data is queued by *Kerio Personal Firewall* in its memory buffer). If the user reacts too slow, the application might consider this status as a network error (server not available) after a certain period (typically a few seconds).

3.3 Starting/Replacing/Launching other application Dialog

The *Starting/Replacing/Launching other application* dialog informs users that *Kerio Personal Firewall* has detected an attempt to startup oan application or to run an application by another one. Decide whether the action will be permitted or denied and whether an appropriate rule will be created. The application will not be opened unless permitted by user.

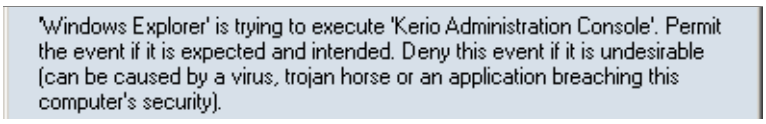
Note: The way how *Kerio Personal Firewall* will behave when applications are started is defined by rules in the *System Security* section (refer to chapter 6). The *Starting/Replacing/Launching other application* dialog is opened if no corresponding rule is found or the rule asks user explicitly.

This dialog is displayed “Always on Top”. Whenever multiple concurrent events (multiple connection attempts or an attempt to open multiple applications at one moment — see chapter 3.3) are detected, these events are queued — the dialogs are opened in turn when a current dialog is answered.



The *Starting/Replacing/Launching other application* dialog provides the following information:

Description A brief description of a particular event and a general recommendation which action should be used are provided in the dialog header.



Note: If description of the application (or the file name if there is no description available) is too long, it will be shortened to 32 only and three dots will be added at the end to inform that the item is not displayed complete.

Name Information on which event type was detected is displayed in the colored field:

- *Starting application* — an application is to be launched
- *Replacing application* — executable file of an application is to be replaced
- *Application is launching other application* — the running application is attempting to launch another application

Icon and application name Icon and description of the application are provided below below the information on application type. If no description is available, name of the executale file is displayed. If the application has no icon, the standard system icon for executable files will be used.

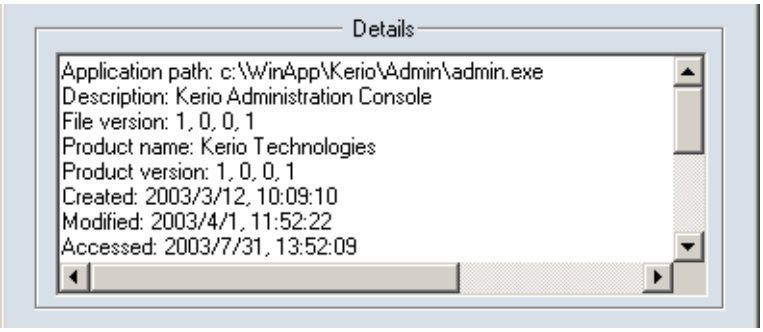
If the application was launched by another application, information on such application will be displayed below (*Launched by*).

Place the mouse pointer over the description on the application or over the description of the application by which it is launched to view a tooltip providing full path to the executable file of the corresponding application.

Action Select an action which will be taken for this application.

- Use the *Permit* button to allow the application.
- Select the *Deny* button to block the application.
- Check the *Create a rule for this event and don't ask me again* option to create a rule (in *System Security / Applications*). Next time this event is detected, the rule will be applied without asking user.
- Click on the *Details* button to view detailed information on the started application (eventually also information about application by which it is launched)

Details Open the *Details* section to view information on the starting application, eventually also information about application by which it is launched (full path to the executable file, description of the application, version number, date when the file was created/modified, the latest date of when the file was accessed, etc.).

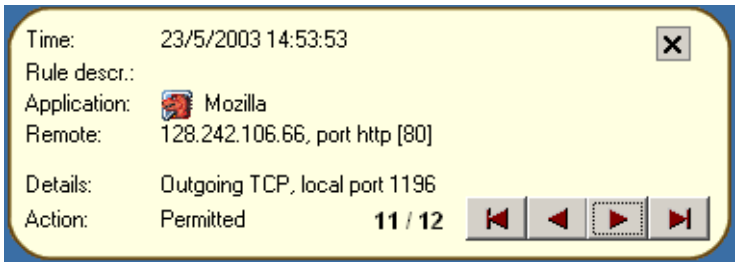


3.4 Alert Dialog Window (alerts on events)

You can enable the *Alert* dialog in *Kerio Personal Firewall* rules or by running a corresponding application. This dialog will appear when a packet is sent or received that meets the conditions of the rule. A window providing information on the connection will be displayed in the right bottom corner of the screen. If other events meeting the rule are detected while this window is open, they will be queued. The queue can be listed in both directions using the arrow buttons.

Warning: If you close the *Alert* dialog (by clicking on the cross button at the right top of the window or using the *Alt+F4* keys), all queued alerts will be removed, regardless of the fact that they have been displayed or not!

Network Connection Alert



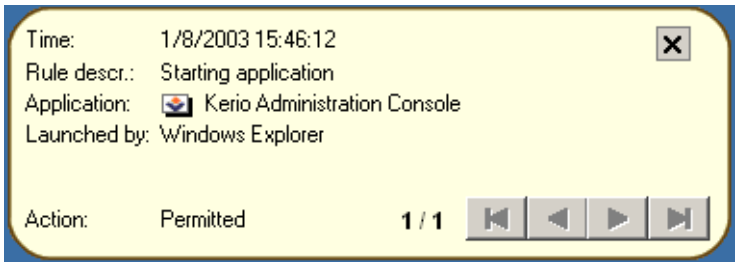
The *Alert* window provides the following information:

- *Time* — date and time when the connection was initiated
- *Rule descr.* — description (name) of a used traffic rule

- *Application* — icon and name of the local application used for the communication (if this application has no icon, a default system icon will be used; if no name is available for the application, the name of the corresponding executable file will be displayed)
- *Remote* — IP address and port of the remote computer (if a name can be identified using DNS, this name will be displayed instead of the IP address; the protocol name will be displayed before the port number for standard services)
- *Details* — connection details: direction (*Outgoing* or *Incoming*), protocol and local port
- *Action* — action which has been taken (*Permitted* or *Denied*)
- sequence number of the alert in the queue (the total count of alerts will grow when new alerts are generated by *Kerio Personal Firewall*)
- buttons to list in the alert queue — function of buttons from left to right: go to the first/previous/next/last alert

For detailed information on network communication rules refer to chapter 5.2.

Example of Starting Application Alert



The *Alert* dialog includes the following items:

- *Time* — date and time of the event
- *Rule descr.* — description of detected event:
  - *Starting application* — an application was started
  - *Replacing application* — replacement of application's executable file
  - *Application is launching other application* — the running application is attempting to launch another application

- *Application* — icon and name of a local application participating in the communication (if no icon is available, the standard system icon will be used; if application name is not available, name of a corresponding executable file without extension will be displayed)
- *Launched by* — name (description) of an application by which the application is launched
- *Action* — action that was *Permitted* by a corresponding rule (starting application *Permitted*/*Denied*).

For details on running application rules see chapter 6.1.

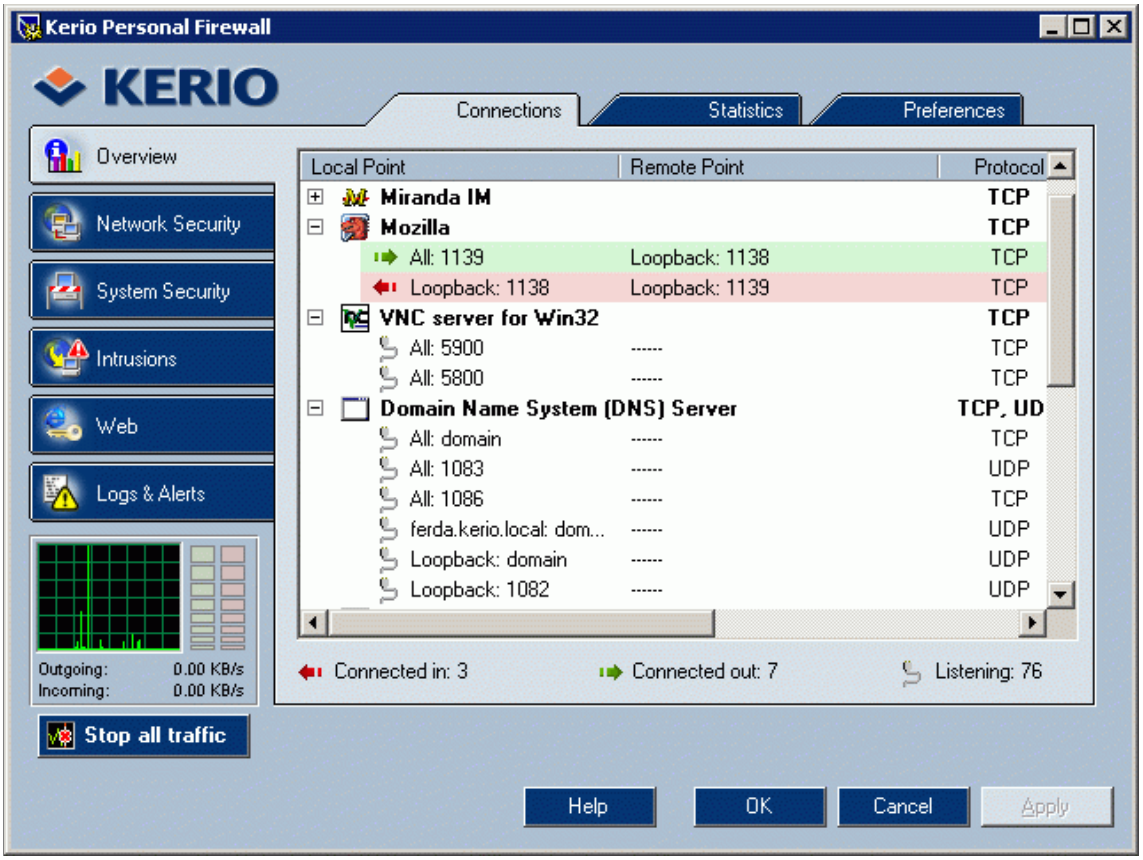
Chapter 4

Firewall Configuration

4.1 Configuration Dialog

Kerio Personal Firewall parameters can be set and status information can be viewed in the configuration dialog. Use one of the following methods to enter this dialog:

- double-click on the *Kerio Personal Firewall* icon located on the Systray
- right-click on the icon and select the *Configuration* option in the context menu



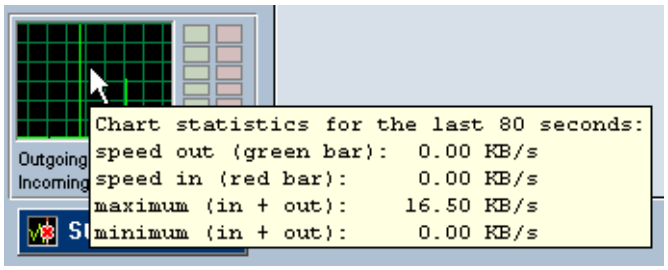
Use tabs on the left to switch between individual sections:

- *Overview* — list of active and open ports (see chapter 10.1), statistics (see chapter 10.2), user preferences. (refer to chapter 4.3)..
- *Network Security* — rules for network communication of individual applications, packet filtering, trusted area definitions (see chapter 5)
- *System Security* — rules for startup of individual applications (read more in chapter 6.1)
- *Intrusions* — configuration of parameters which will be used for detection of known intrusion types (see chapter 8)
- *Web* — Web content rules (URL filter, pop-ups blocking, control over sent data — see chapter 9)
- *Logs & Alerts* — logs viewing and settings (refer to chapter 11)

Chart at the bottom of the dialog window shows traffic load of a particular network interface. The green bar next to the chart represents current speed of outgoing traffic, whereas the red bar shows current speed of incoming traffic.

Click on the chart to switch between the line graph and the bar graph.

Place the mouse pointer over the chart to view a tooltip giving statistics of network traffic:



- *speed out (green bar)* — current speed of outgoing traffic
- *speed in (red bar)* — current speed of incoming communication
- *maximum (in+out)* — top speed record
- *minimum (in+out)* — bottom speed record

Use the *Stop all traffic* button to block all network traffic (all connections will be stopped immediately). This function can be helpful for example when communication which

was supposed to be denied has been permitted by mistake. If this option is used, it is replaced by the *Enable traffic* option.

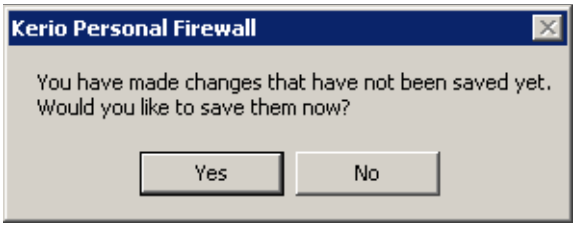
If traffic is stopped, this will be shown by the icon and the *Enable traffic* text below the button.

Note: The *Stop all traffic / Enable traffic* option is also available from the context menu called through the *Kerio Personal Firewall* icon displayed on the Systray (refer to chapter 2.2).

Buttons at the dialog bottom provide the following functions:

- *OK* — saves all changes and closes the configuration dialog
- *Cancel* — closes the dialog without saving changes
- *Apply* — saves and applies all changes and leaves the dialog open

Note: Changes in configuration can be done in only tab of one section at a time. If you attempt to switch to another tab or to another section, the system seeks possible changes that could have been made since the last save. If some changes are detected, *Kerio Personal Firewall* asks users whether they should be saved or canceled.



Protected Configuration

It is possible to set *Kerio Personal Firewall* configuration so that it can be accessed only through a password authentication (only authorized users are then allowed to modify settings). In such case unauthorized users are allowed only to view the configuration. Password will be required if a configuration change is attempted.

After insertion of a correct password a particular user will be logged-in. This user will be authorized to change the configuration.

We recommend authorized users to logout after the desirable changes are done so that no unauthorized user can modify the configuration. Use the *Logout* option in the context menu accessible through the icon in the Systray (see chapter 2.2), or the *Logout* button in *Overview / Preferences*. If a user does not log out, the configuration can be accessed and modified unless the *Personal Firewall Engine* service is closed.

4.2 Remote Administration

Kerio Personal Firewall can be also administered remotely (from a remote station — not from the one where the *Personal Firewall Engine* service is running). Two alternatives of remote administration are available:

- access to the configuration — all settings and functions available through the configuration dialog can be accessed from a remote computer. Dialogs during events (initialization of applications, network communication) and notifications on events can be viewed only through the computer where the *Personal Firewall Engine* is running.
- session is redirected — all dialogs and notifications will be also redirected to a particular remote station.

Access from a remote workstation

The following steps must be followed for a successful remote access to the *Personal Firewall Engine*:

1. Allowing remote administration and setting a password which will be used for access to the administration

   Remote access to the *Personal Firewall Engine* is available only through a successful user authentication (password request). Enable the *Enable password protection* and

the *Allow remote administration of this computer* options in the *Overview / Preferences* section. Set a password if not specified yet. For details refer to chapter 4.3.

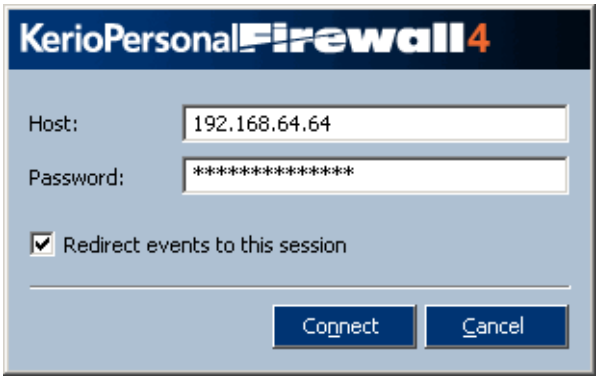
2. Running the *Personal Firewall GUI* at a remote computer

   - If *Kerio Personal Firewall 4.x* is installed on the remote computer, select and run the *Remote Firewall Administration* from the *Kerio* program group.

   - If *Kerio Personal Firewall* is not installed on the remote computer, copy the `kpf4gui.exe` file or the `trans` subdirectory (if you intend to use another language version of the interface than the English one) from the local workstation (typically from the `C:\Program Files\Kerio\Personal Firewall 4` directory) and run it on the remote workstation.

3. Authentication to access the *Personal Firewall Engine*

   Use one of the methods of running *Personal Firewall GUI* described above to open the authentication dialog where you can login to the *Personal Firewall Engine*.



Address DNS name or IP address of the computer on which the *Personal Firewall Engine* is running. After a successful connection this name or the IP address will be displayed:

- in the header of the configuration window

- in tooltip accessible through the icon on the Systray

Password Password through which the administration can be accessed (see step 1).

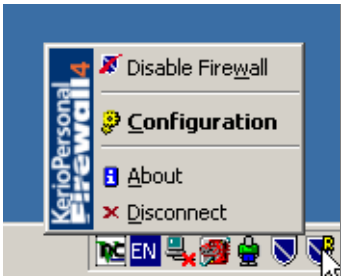
Redirect events to this session Check this option to redirect all dialogs and notifications to the remote computer.

This option enables thorough control of the *Kerio Personal Firewall* from a remote computer. It is not recommended to use this option if you want to perform a single-shot modification of the configuration.

Click on the *Connect* button to establish connection with a remote workstation.

Note: Connection to a remote administration is allowed by the internal *Kerio Personal Firewall* policy. This means that it is not necessary to define special network security rules to enable remote administration.

When connected successfully to the *Personal Firewall Engine*, the *Kerio Personal Firewall* icon with a symbol of remote connection (*R* — remote) is displayed in the System Tray. The context menu provides the following functions:



Disable firewall Deactivates the firewall (all security functions are disabled).

Configuration Use this option to enter the configuration dialog where all settings which are available on the local host can be done (except for disabling of network communication). For details see chapter 4.1.

About Information about versions of individual *Kerio Personal Firewall* components as well as license of the firewall and expiration date in case of a trial version (the same information which is provided when a user is connected locally).

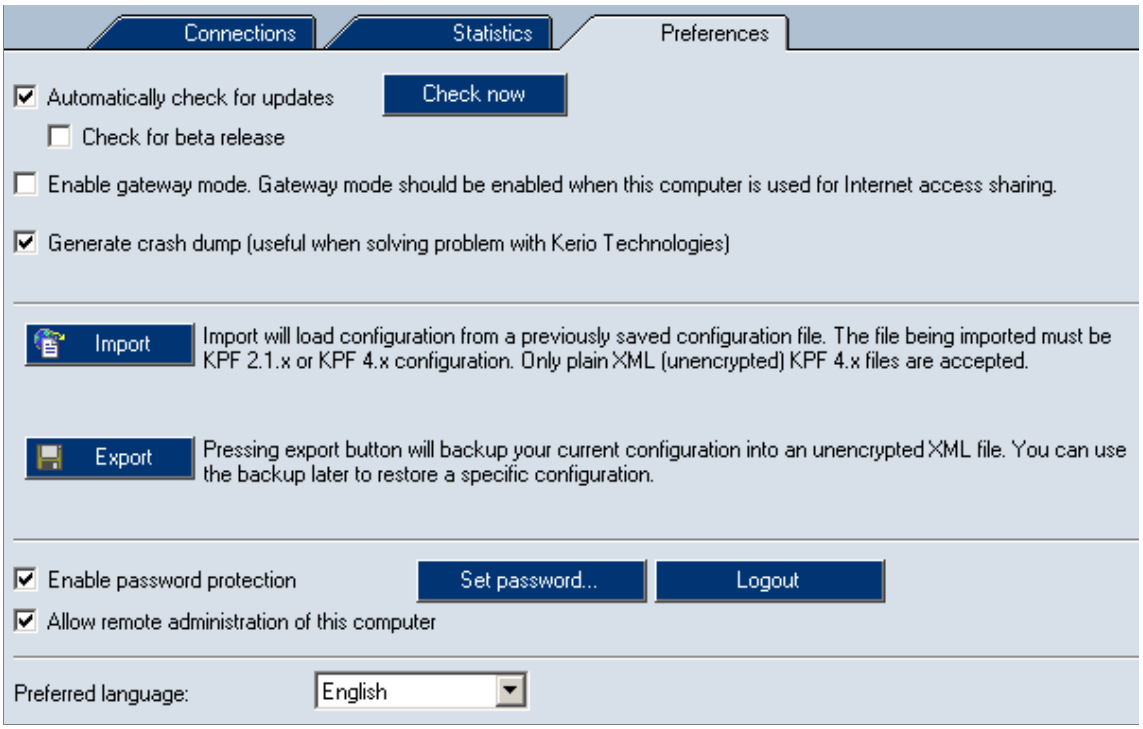
Disconnect Disconnection from the remote *Personal Firewall Engine* administration and closing the *Personal Firewall GUI* on the computer from which the remote access has been performed.

Note: Unlike in case of local administration, the following functions are not available for remote connections:

- *Stop all traffic* (this function would block connection of the *Personal Firewall Engine* with the *Personal Firewall GUI* operating on the remote host)
- *Logout* (users must be authenticated to be allowed to administer the firewall remotely and they will be logged out automatically when disconnected from the *Personal Firewall Engine*)
- *Exit* (the *Personal Firewall Engine* service cannot be closed remotely; the *Personal Firewall GUI* running on the remote host can be closed using the *Disconnect* option)

4.3 Preferences

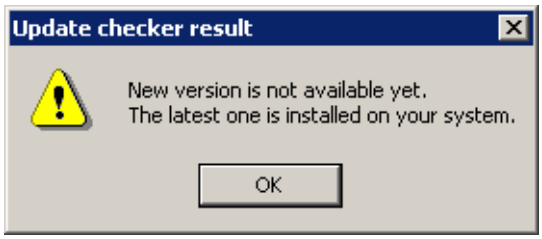
User preferences and advanced firewall parameters can be set in the *Overview / Preferences* section.



Automatically check for updates Enables/disables automatics checks for new versions. We recommend to enable this option to provide maximal security (new versions include updates of intrusion database, bugs are removals, etc.).

For detailoed information on automatic checks and installation of new versions refer to chapter 1.6.

Check now Use this button to check for new version of *Kerio Personal Firewall* immediately. If a new version is found at the update server, download and instalation will be offered (for details see chapter 1.6). If not, user will be informed that no new version is available (the latest version is already installed at the computer).



Check for beta release Enable this option to perform checks for released beta versions along with checks for new full versions. Beta versions are program versions the are just being developed and tested. Therefore, their smooth functionality is not guaranteed and bugs may occur.

Use the *Check for beta release* option if you intend to participate in product testing for details refer to `http://www.kerio.com/`, *Beta Sections*). If you are not interested in the participation and you want to use a functioning version, disable this option.

Enable gateway mode This option switches the firewall to a special mode — protection of the Internet gateway (the firewall will run on router or NAT router).

If this option is selected, *Kerio Personal Firewall* will let through packets with destination ports at which no local application is running, or packets with destination IP addresses which are not local.

Do not use this option unless *Kerio Personal Firewall* is really ranning on the Internet Gateway, otherwise protection of the local computer might be seriously reduced!

Notes:

1. The *Enable Gateway Mode* option can be also used to allow communication of the operating system which is run within *VMWare* (`http://www.vmware.com/`) if *Kerio Personal Firewall* protects host system. If this option is disabled, *Kerio Personal Firewall* will block all packets routed to the operating system within the *VMWare*.

2. If *Kerio Personal Firewall* is used for proxy server protection, it is not necessary to enable this option (proxy server behaves as a client on the local computer).

Generate crash dump Use this option to enable generation of debugging information which could be used after a possible *Kerio Personal Firewall* crash . If the *Personal Firewall Engine* or the *Personal Firewall GUI* crashes and this option is available, a file including memory data will be created and the *Assist* utility which enables to send crash information (compressed memory information and selected logs) to *Kerio Technologies* (for analysis) will be launched automatically.

Note: No user data (nor memory data created by the operating system) is sent to *Kerio Technologies*.

Crash dump is sent in a compressed format. Content of the following system registry path will be also packed to this file:

`HKEY_CURRENT_USER\Software\Kerio\Personal Firewall 4`.

Notes:

1. If the operating system crashes, *Kerio Personal Firewall* can send core memory data (full memory data in case of Windows NT 4.0) for analysis after new startup. A check whether a new memory data file is available on the disc is provided one minute after the *Personal Firewall Engine* service is started. If so, the *Assist* utility is launched. This utility asks user whether the crash was caused by the firewall or not. If the answer is Yes, delivery of information for later analysis to *Kerio Technologies* will be offered. The memory data file is sent in a compressed format.

2. Any received information will be used only for *Kerio Personal Firewall* debugging. It will not be used for another purpose nor it will be passed on to other parties

Configuration This section provides functions for *Kerio Personal Firewall* back-up, its recovery and *Kerio Personal Firewall 2.1.x* configuration backup restoration.

Use the *Import* button to open the file. *Kerio Personal Firewall* can open and download configuration file in the following formats:

- *Kerio Personal Firewall 4.x* unencrypted (the XML format with the `.cfg` extension)
- *Kerio Personal Firewall 2.1.x* (with the `.conf` extension) — import of older configuration (back-up)

Click on the *Export* button to save the file. This way you can back-up the unencrypted configuration file for later use or for its use on another computer.

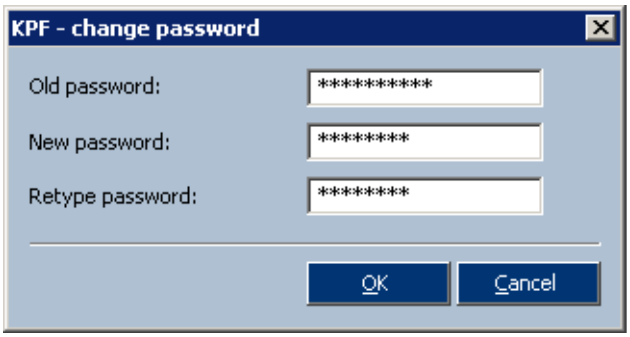
Note: Encrypted configuration files cannot be imported.

Enable password protection Set password which will be used to access the *Kerio Personal Firewall* configuration. If the configuration is password protected, it can be

only viewed. Users are allowed to change configuration after a successful password authentication. For detailed information refer to chapter 4.1.

Users can log out using the *Logout* button — password will be required before further changes. It is also possible to log out through the context menu which can be found in the Systray (see chapter 2.2)

Click on the *Set password...* button to open a dialog where password can be edited.



Insert your current password into the *Old password* entry (only authorized users are allowed to edit password). This entry is inactive if not defined yet (after the *Kerio Personal Firewall* is installed, when the configuration is removed, etc.). Use the *New password* entry to specify a new password and conform it using the *Retype password* entry.

Note: Remote administration of the *Kerio Personal Firewall* is available only to user-sauthenticated through the password. If the *Enable password protection* option is disabled, remote administration cannot be enabled (the following option is not available).

Allow remote administration of this computer Use this option to enable an internal firewall rule which allows connection to the *Kerio Personal Firewall* administration from a remote station (see chapter 7.1). Remote administration is disabled by default.

For detailed information on remote administration refer to chapter 4.2.

Preferred language Select preferred language for the *Kerio Personal Firewall* user interface. Click on the *OK* or the *Apply* button to restart the interface. Next time the configuration dialog or the context menu is opened, this language will be used.

Language versions (localizations) are available in the `trans` subdirectory in the directory where the *Kerio Personal Firewall* is installed. The *Personal Firewall Engine* detects which language versions are available and then any language version can be selected from the *Preferred language* menu.

Preffered language also affects selection of the most relevant help file. If no corresponding help file for the language is found, *Kerio Personal Firewall* will attempt to open the English help file automatically. If not even the English version is detected, help file will not be opened.

Notes:

1. Help files are saved in the directory where *Kerio Personal Firewall* is installed. Context help files are provided in the *Microsoft HTML Help* format and they are called `kpf4-<language_abbreviation>.chm` (`language_abbreviation` is a language name represented by two characters)

2. If *Kerio Personal Firewall* finds out that a particular localization file does not correspond with the current version of the user interface, user will be informed about this fact by an alert. This fact would not affect functionality of the firewall, however, some texts and labels may not be up-to-date or provided only in English.

Chapter 5

Network Security

The most important part of the *Kerio Personal Firewall* configuration is definition of network communication rules. The following three rule types are available:

- *Rules for applications* — simple rules defining how the firewall will behave during network communication in trusted areas and in the Internet. These rules are generated automatically. This process is based on the user's reactions to dialogs regarding unknown network traffic. For details see below.

- *Advanced Packet Filter* — detailed rules for network communication (optional configuration of IP addresses, protocol, ports, application,etc.). Rules for packet filters can be either defined by hand in the *Kerio Personal Firewall* configuration dialog or generated automatically according to user's reactions to connection alerts (for details refer to chapter 3.2)

  Advanced packet filter configuration is described in detail in chapter 5.5.

- *Predefined network security rules* — *Kerio Personal Firewall* includes set of predefined rules which are independent from individual applications. For these rules, only actions which will be taken can be set (allow or deny rule). Predefined rules can be either enabled or disabled (one ption for all the rules). For details refer to chapter 5.3.

  The network security module can be enabled/disabled through the *Enable Network Security module* option in the *Applications* tab of the *Network Security* section. If the option is unchecked, all described rule types are unavailable.

5.1 How the Firewall Policy is Applied

When a particular communication is detected, individual firewall modules apply rules one by one in a defined order. If the communication meets a rule, ac orresponding action will be taken and no more rules will be tested.

Rules of individual *Kerio Personal Firewall* modules are applied as follows:

1. Intrusion detection system (IDS — refer to chapter 8)

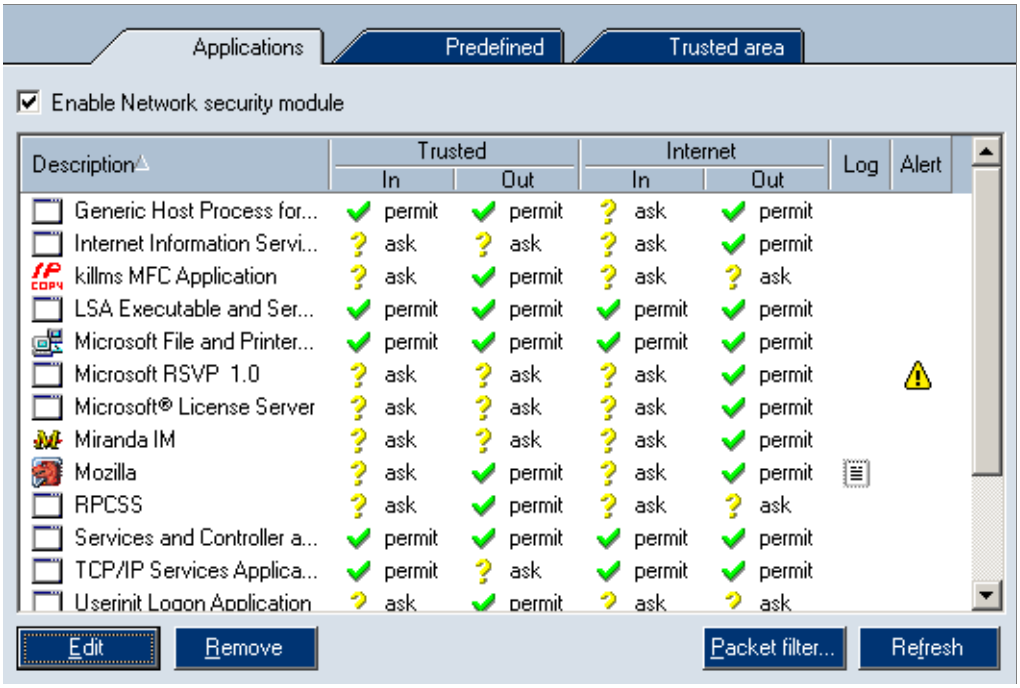
2. Internal rules for *Kerio Personal Firewall* components — i.e. permission to access a web server in order to check and download new versions of the program

3. Advanced packet filter rules (see chapter 5.5)
4. Predefined network security rules (see chapter 5.3)
5. Application rules (more information in chapter 5.2)

Note: Individual firewall components may be disabled — corresponding rules will not be applied on detected communication. Internal firewall rules cannot be switched off.

5.2 Rules for Applications

Rules for applications can be viewed and modified in the *Applications* tab of the *Network Security* section.



Each rule is defined by the following items:

Description Application icon and description. If an application has no icon, a system icon for executable files will be used. If no description is available for an application, the name of its executable file (without extension) will be displayed.

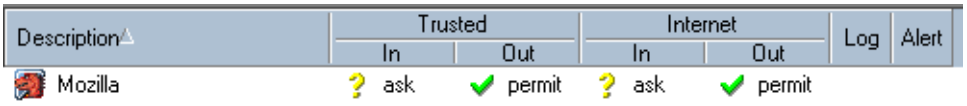
Note: Icons and descriptions of applications cannot be edited in *Kerio Personal Firewall*.

Trusted, Internet Setting of parameters for how a particular application will behave during connection from/to a *Trusted* area or from/to the Internet (*In* — incoming connection; *Out* — outgoing connection).

For each zone and direction one of the following actions can be selected:

- *permit* — allows the connection
- *deny* — blocks the connection
- *ask* — *Kerio Personal Firewall* asks the user to either permit or deny the connection. Anytime a new connection is detected, the *Connection Alert* dialog is opened (for a detailed description of this dialog read chapter 3.2) and the user decides how the firewall will react.

  Note: Rules can be edited in the *Connection Alert* dialog using the *Create a rule for this communication...* option. If this option is checked, the default *Ask* action is switched to an action selected by the user.



Example: Rule for the *Mozilla* Web browser — see the screenshot above

Web browsers are typical client applications which connect to Web servers. Outgoing connection (*Out*) from these applications can be permitted (*Permit*). Because Web servers do not open a connection to the client, we can *Deny* incoming connections for *Mozilla* or we set the *Ask* action so that such connection attempts will be always reported and the firewall will ask the user to take an appropriate action.

Log Check this option to log all communication which would meet the rule into the *Network* log (see chapter 11.4), regardless of the action which has been taken (both permitted and denied connections will be logged).

Alert Check this option if you want *Kerio Personal Firewall* to display an alert anytime a connection meeting this rule is detected. The message will appear in the *Alert* dialog window (refer to chapter 3.4), regardless of whether the connection is permitted or denied.

This function can be helpful for example when a connection is denied and we want to find out when the remote points repeat the connection attempt.

Use the *Edit* button to edit a selected rule (see below). Use the *Remove* button to remove a selected rule. The *Refresh* button can be used to refresh the rule list (when the *Applications* tab is open, an interaction between the firewall and user may arise and rules may be added or modified).

Default Rule

The *Another application* rule (so called default rule) is always placed at the end of the list of network traffic rules for applications. This rule applies to network traffic which does not match with any other rule.

In the default rule, the *Ask* action is set as default for both incoming and outgoing traffic — if no application rule matches with a connection attempt, *Kerio Personal Firewall* asks users whether the particular connection will be permitted or denied, and whether or not a rule for such communication will be created (see chapter 3.2). Actions can be changed to create various rules, such as "deny traffic for all applications to which no rule applies", "permit traffic for all applications to which no rule applies, but in the trusted area only" etc.

Default rule is highlighted in the rule list. It cannot be removed.

Options

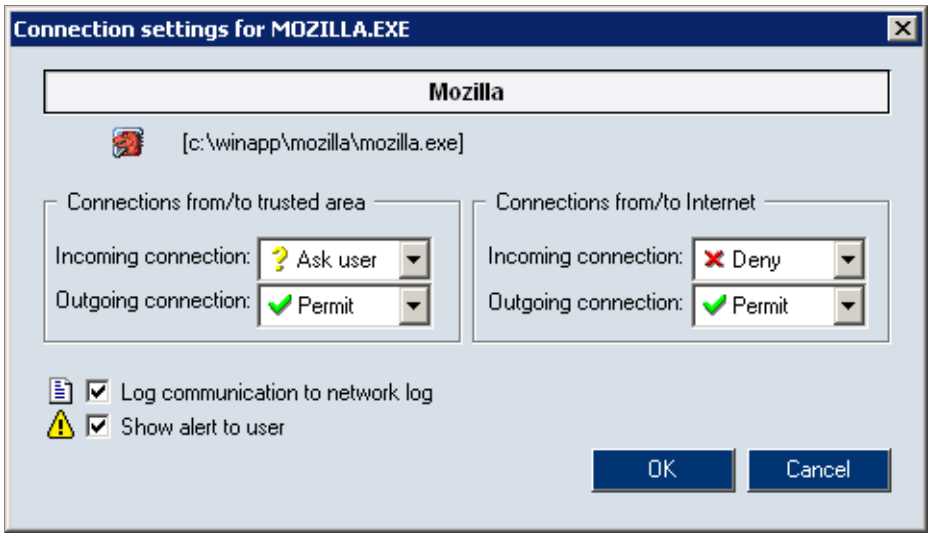
The folowing options are available for the rules:

1. Right-click on the *Description* column to open the context menu providing the following functions:
   - *Edit* — opens a dialog where a selected rule can be edited(see below)
   - *Remove* — removes a selected rule
   - *Displayed application name* — use this option to define how the application name will be displayed:
     - *Full path* to the file
     - *File name* without the path
     - *Description* of the application

     Use the *Show icon* option to enable/disable application icons before application names or descriptions.
2. Click on an action (in the *Trusted* or the *Internet* column):
   - left-click to switch between the *Permit*, *Deny* and *Ask* actions
   - right-click to open a context menu and select an action.

Edit

Click on the *Edit* edit button in the context menu to modify a selected rule. In this dialog you can set actions for individual zones and traffic directions, logging and parameters for sending alerts to users.



Description of an application is displayed at the top of the dialog. Below this description, icon and full path to the application executable file is given. This information cannot be edited.

In the center of the dialog window actions for individual zones and traffic directions can be set.

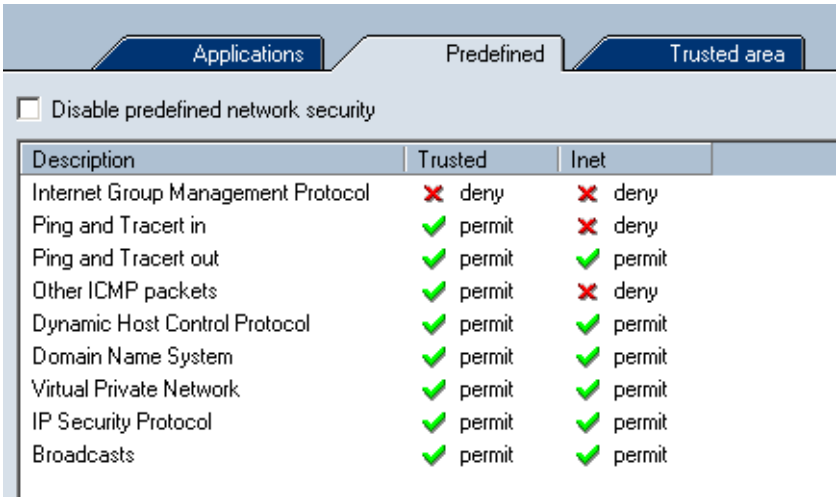
Check the *Log communication to network log* option to enable logging of communication meeting this rule to the *Filter* log (see chapter 11.4).

Use the *Show alert to user* option to enable the *Alert* dialog (refer to chapter 3.4) for connections meeting this rule.

5.3 Network Security Predefined Rules

Kerio Personal Firewall includes several predefined rules. These rules are independent from individual applications (they are applied globally). User decides whether individual predefined rules will be used or not. These rules can be modified.

Predefined rules for network traffic can be found in the *Predefined* tab of the *Network Security*section.



Rules in this tab cannot be added nor removed. Actions for *Trusted* area and the Internet can be set for each rule. To switch between actions (*Permit*/*Deny*) click on a corresponding field.

Note: The *Ask* action (asking user whether the traffic will be allowed or not — see chapters 5.2 and 3.2) is not available for predefined rules.

Check/uncheck the *Disable predefined network security* option to disable/enable predefined rules for network communication. If this option is checked, predefined rules are ignored and *Kerio Personal Firewall* uses only application rules (see chapter 5.2) and advanced packet filter rules (see chapter 5.5).

Use the *Set to defaults* button to restore actions for predefined rules to default values.

Predefined Rules

Brief descriptions on predefined network security rules are provided in this section.

Internet Group Management Protocol The *IGMP* used for subscription or unsubscribtion to/from groups of multicast users. This protocol can be misused easily and that is why it is disabled by default. We recommend you not to enable this protocol unless you run applications which use multicast technologies (typically for transmission of audio or video data through the Internet).

Ping and Tracert in, Ping and Tracert out Programs *Ping* and *Tracert* (*Traceroute*) are used to trace route in a network (to detect response of a remote computer). This is achieved through messages of *ICMP* (*Internet Control Message Protocol*).

First, a possible attacker tests whether as elected IP address responds to control messages. Blocking these messages will make your computer "invisible" and reduces chance of possible intrussions.

All incoming *Ping* and *Tracert* messages (from the Internet) are blocked by default. These messages are allowed from the trusted area (administrator can for example test availability of a computer by the *Ping* command).

Outgoing *Ping* and *Tracert* messages are permitted for both areas. These methods are usually used to verify network connection functionality or avalability of a remote computer.

Other ICMP packets Rule for other *ICMP* messages (i.e. redirections, destination is not available, etc.)

Dynamic Host Configuration Protocol *DHCP* is used for automatic definition of TCP/IP parameters (IP address, network mask, default gateway, etc.).

Warning: DHCP denial might cause that network connection of your computer will not work if TCP/IP parameters are defined through this protocol.

Domain Name System *DNS* is used for translation of computer names to IP addresses. At least one connection to a DNS server must be permitted to enable definition through DNS names.

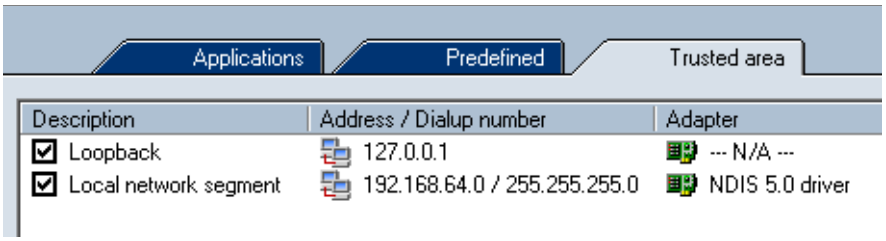
Virtual Private Network Virtual private network (VPN) is a secure connection of two local networks (or connection of a remote client to a local network) via the Internet using an encrypted channel (so called tunnel). The *Virtual Private Network* rule controls VPN establishment through the *PPTP* and *IPSec* protocols.

Broadcasts Rules for packets with general address. In the Internet, this rule is also applied on packets with multicast addresses.

5.4 Trusted Area Definition

Two types of IP groups are distinguished for *Kerio Personal Firewall* application rules: trusted area and the Internet. Separate actions for incoming and outgoing traffic can be defined for each area. *Trusted area* is a user-defined IP group. Address which are not defined as trusted will be added to *Internet* zone automatically.

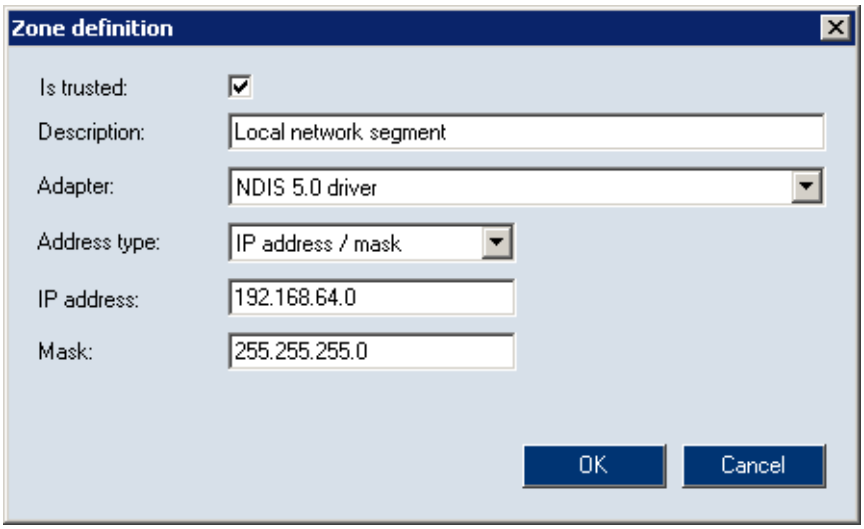
To define your trusted area go the *Trusted area* tab in the *Network Security* section.



Trusted area can include any number of IP addresses, IP address ranges, subnets or networks connected to a particular interface (for details read below). It is possible to specify interface on which particular IP addresses are permitted for each item (protection from false IP addresses).

Trusted area includes the predefined *Loopback* item. This item cannot be removed. It is a local loopback address and it is always considered trusted.

Use the *Add* or the *Edit* button to define an item of the trusted area (or double-click on a selected item to *Edit* it).



Is trusted Use this option to add/remove a selected item to/from the trusted area. If the *Is trusted* option is not checked, the IP addresses (IP ranges, subnets, etc.) do not belong to the trusted area (and they are added to the *Internet* zone automatically).

The *Is trusted* option can be used for example for explicit specification of IP addresses which do not belong to the trusted area. *Kerio Personal Firewall* will be aware of a corresponding interface and it will not ask user when traffic at this interface is detected (see chapter 1.7).

Description Item description. For reference only.

Adapter Select an adapter (interface) for which the IP addresses are used. This function protects users from false IP addresses — whenever a packet with a trusted address is received from an adapter which is not connected into the particular network, the packet is considered untrusted.

Use the — *Any* — option if you want that *Kerio Personal Firewall* does not check adapters from which packets with a particular IP address was sent.

Address type Type of a trusted area item:

- *Computer* — a particular IP address of a computer (or a network device)
- *IP address / mask* — subnet defined by IP address and mask of the network
- *IP address / range* — IP range defined by first and last IP address
- *All addresses* — any IP address

Note: The *All addresses* option can only be used with a particular adapter ("network connected to this interface"). If it had been possible to combine this option with the — *Any* — option in the *Adapter* item, all IP addresses would have belonged to the trusted area. This would be irrelevant and such setting is not allowed by *Kerio Personal Firewall* (the *OK* button is not active).

5.5 Advanced Packet Filter

The packet filter allows for definition of advanced rules for specific network communication. Besides selection of a local application and traffic direction, protocol, remote IP addresses, remote and local ports and other parameters can be defined.

Rules for packet filter can be defined as follows:

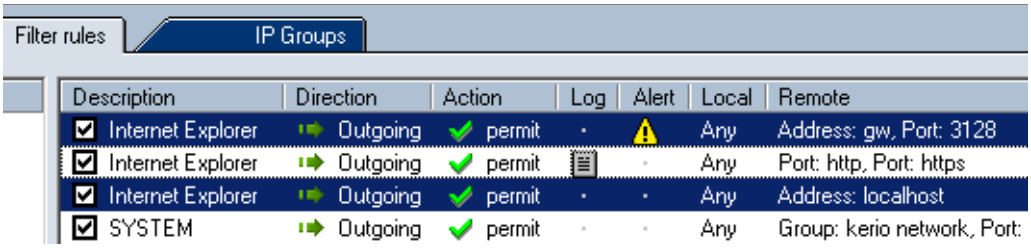
- By hand — click on the *Packet Filter...* button in the *Applications* tab of the *Network Security* section to open the *Advanced Packet Filter* dialog where packet filter rules can be viewed, edited and removed (for details see below).
- Automatically — the *Connection Alert* dialog is opened when aconnection which does not meet any rule is detected (see chapter 3.2); if the *Create an advanced filter rule* option is checked,a packet filter rule will be created instead of a standard rule.

Note: Advanced packet filter does not distuinguish between trusted area and the Internet (an IP address, subnet, IP group, etc. are always specified in the rule).).

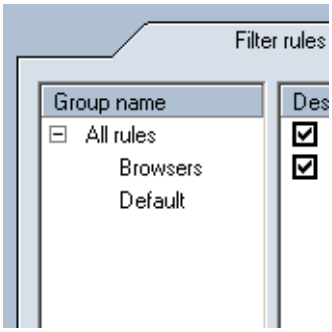
Packet Filter Rules

Rules for advanced packet filters can be viewed in the *Filter Rules* tab of the *Advanced Packet Filter* dialog window.

Rules are ordered in a list. Anytime a network connection is detected, the list is tested rule by rule from the top downwards and the first rule whcich the traffic meets is applied. Use the *Up* and *Down* buttons or *Ctrl + up arrow* and *Ctrl + down arrow* key combinations to reorder the list according to your liking and needs. More complex combinations of filtering rules can be defined thanks to these features.



Packet filter rules can be optionally classified by groups. Participiation of a rule in a group does not influence the system of rule appliance since rules in all groups are always tested. This implies that these groups are for reference only. Rule groups are displayed on the left of the *Filter Rules* tab.



Click on a group name to view the list of rules included in the group.

The following two groups are predefined and they cannot be removed:

- *All rules* (“parent group”) — includes all packet filter rules
- *Default* — includes all rules which have not been added into another group.

Note: Groups of rules cannot be created nor removed explicitly. New groups can be created by entering a new group name during a rule definition. Groups are removed automatically when the last rule is removed.

Use the following buttons below the group list to handle packet filter rules:

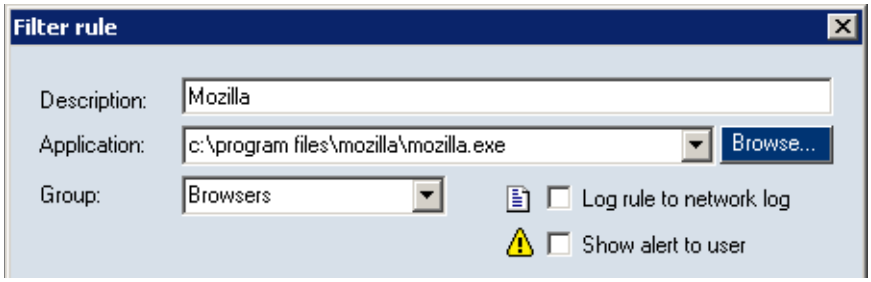
- *Edit* — opens dialog for modification of a selected rule (this dialog can also be opened by double-clicking on a selected rule)
- *Add* — adds a new rule to the end of the list
- *Insert* — inserts a selected rule to the current position (this rule will precede a marked rule)
- *Remove* — removes a selected rule

Notes:

1. If no rule is selected, only the *Add* button is available.
2. Hold down the *Ctrl* or the *Shift* key to select multiple rules. Groups of rules selected in this way can only be moved or deleted. Use the *Edit* button to edit the first selected rule (at the top). The *Insert* button inserts a new rule before the first rule of a particular group.

Rule Definition and Modification

Clicking on the *Add*, *Insert* or *Edit* button opens a dialog for definition of a packet filter rule. A rule is defined by the following parameters:



Description Rule description/name. We recommend you to insert a brief rule description (purpose, application name, etc.). This description is used for your reference only. The name of a particular local application which participates in the communication is inserted for automatically generated rules.

Application Local application to which the rule is applied. This application can be either inserted by hand (full path to a corresponding executable file), selected from a menu (menu of applications used for other rules is offered) or searched on the disc

(use the *Browse...* button to open a standard system dialog from which an application can be run).

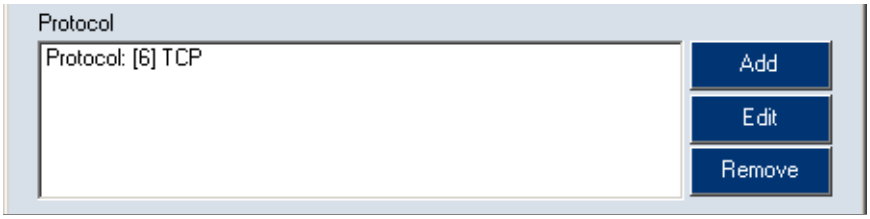
You can also create a general filtering rule which will be applied on all applications. This can be done through the *any* option or by leaving the *Application* item blank.

Group Rule group in which the rule will be included. Participation of a rule in a group does not influence the system of rule appliance — the entire rule list is always tested. This implies that these groups are used for reference only.

Use the *Group* item to choose a group from the menu or to add a new group by inserting a new group name — the rule will be automatically included to this group. All rules are added to the *Default* group by default. The same method is applied on rules which are generated automatically (see above or refer to chapter 3.2).

Log rule to network log Enables/disables logging of communication meeting this rule into the *Network* log (see chapter 11.4).

Show alert to user Check this option to enable the *Alert* dialog (read more in chapter 3.4) whenever traffic meeting this rule is detected.



Protocol Set parameters for protocols to which the rule will be applied. Typically, a single protocol is used for traffic (i.e. TCP or UDP, however, some applications use multiple protocols concurrently (i.e. TCP and UDP using the same ports).

If we leave the *Protocol* entry empty, the rule will be applied to any protocol.

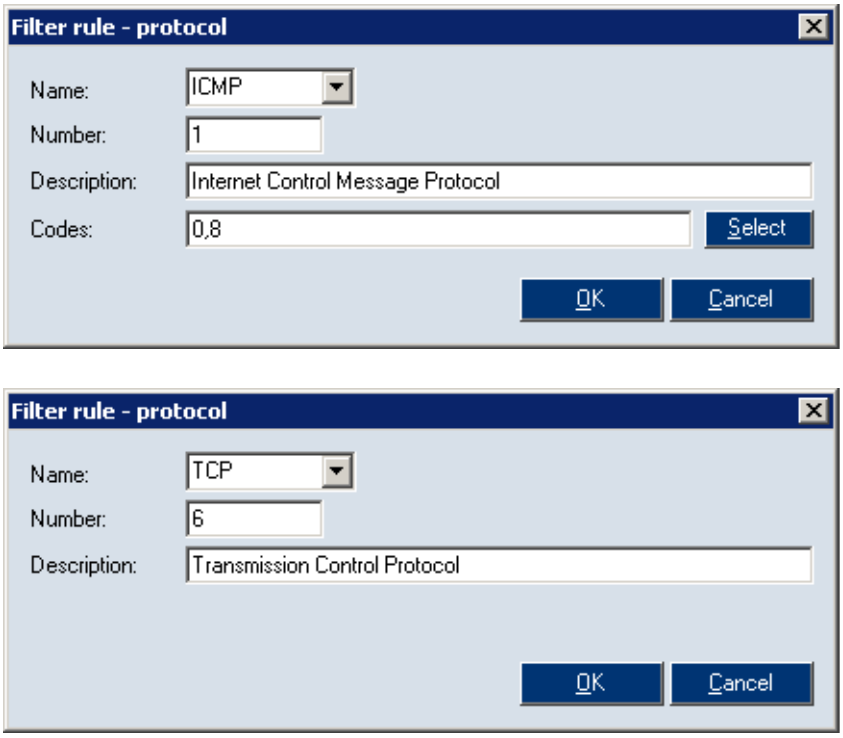
Note: If an application uses TCP and UDP protocols at various ports, two different packet filter rules must be defined.

Click on the *Add* or *Edit* button to open a dialog for protocol definition.

The protocol is specified by a designated number in the IP packet header. This number can be defined directly through the *Number* entry. Use the *Name* option to select from a menu of predefined protocols.

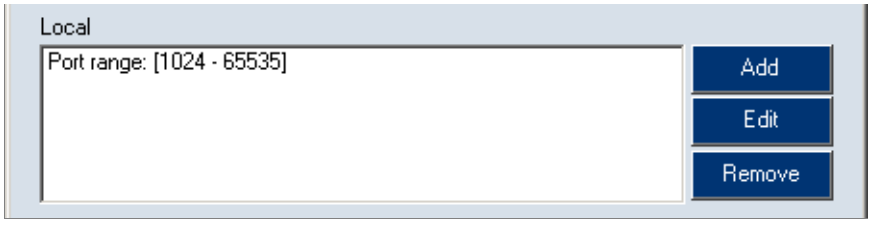
You can use the *Description* textfield to enter a description for your reference. It can be viewed in this dialog only.

The *Codes* item will be available in the dialog if ICMP is selected. Use this entry to specify type of ICMP messages which the rule will be applied on.



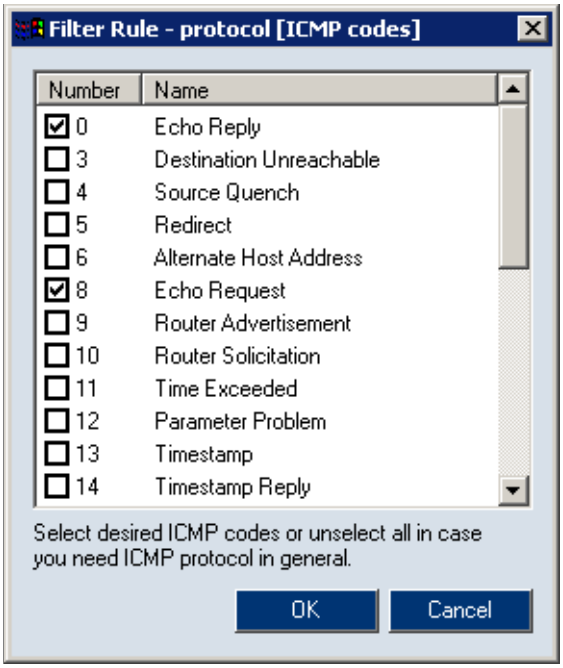
Types of messages are defined by number codes (individual codes are separated by comas). If the *Codes* entry is not specified, the rule will be applied on all types of ICMP messages.

Click on the *Select* button to open a special dialog for definition of types of ICMP messages. Select appropriate types of ICMP messages. Click on the *OK* button and codes of the types you have defined will be inserted into the *Codes* entry automatically.

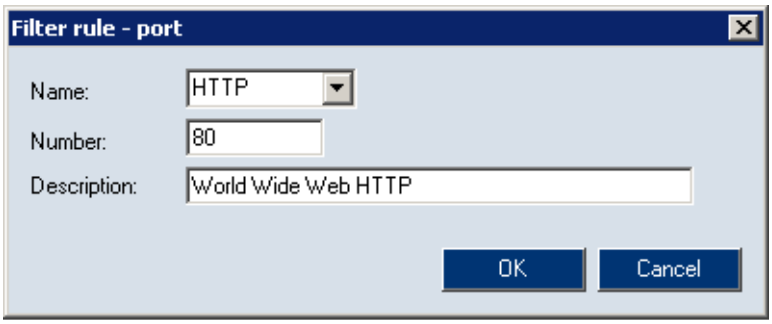


Local Specify parameters for the local point. *Kerio Personal Firewall* uses all local IP addresses implicitly including the loopback IP addresses. For this reason local parameters can be specified only by ports.

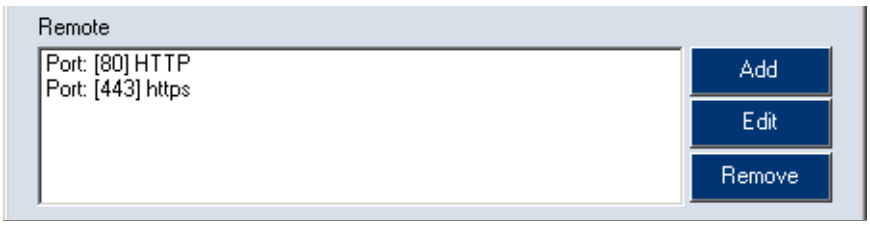
Use the *Add* button to add a single port (*Add port*) or a port range (*Add port range*). Multiple ports and port ranges can be specified — this way any port group can be covered easily.

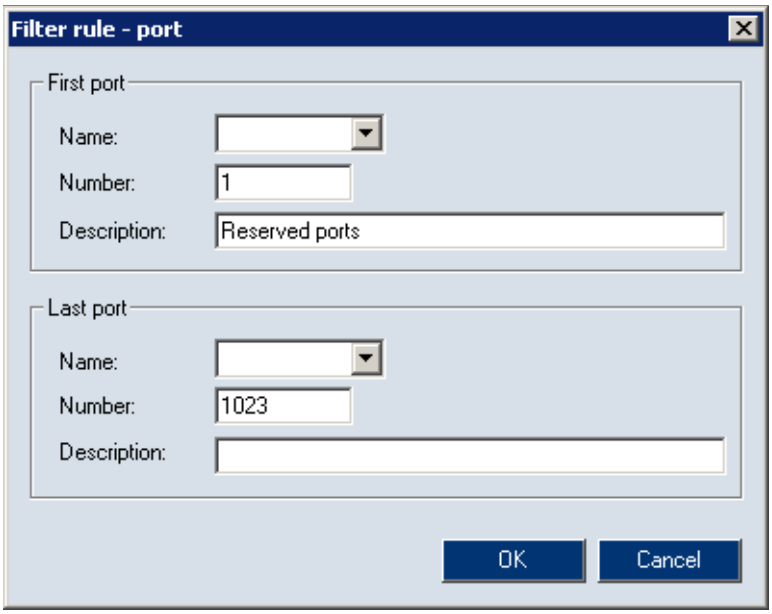


The port can be specified either by specification of the *Number* entry (only values included in the `1-65535` are valid) or by selection of a predefined service in the *Name* item. You can use the *Description* entry to describe the port or the service (for reference only).



The dialog for range specification consists of two essential entries: *First port* (first port in the range) and *Last port* (last port in the range).



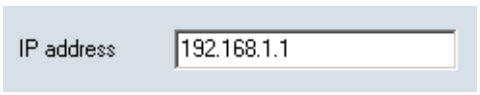


Remote Specification of remote point of a connection. IP address, port or both can be specified. The rule will be applied if the packet will contain any of defined IP addresses and one of the defined ports.

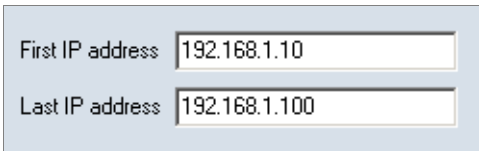
Either individual ports (*Add port*) or a port range (*Add port range*) can be defined. The dialog is the same as for the *Local* point — see above.

Use the following methods to specify IP address:

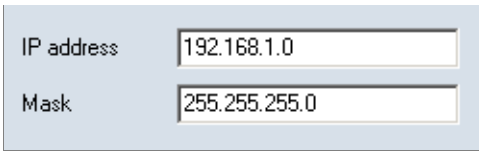
- a single IP address (*Add address*)



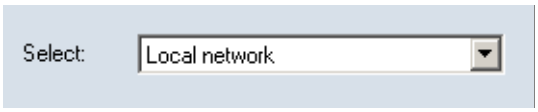
- IP address range(*Add address range*) — enter first and last address of the range



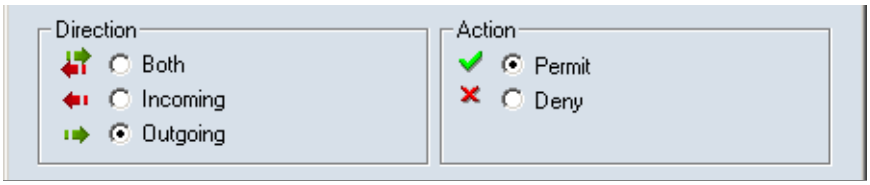
- subnet (*Add address / mask*) — specify subnet address and a corresponding mask



- IP address group (*Add IP group*) — use the *Select* option to select one from the menu of IP addresses defined through the *IP Groups* tab (see below)



Individual methods can be combined.



Direction Direction of the traffic which the rule will be applied to: *Both* directions, *Incoming* or *Outgoing* connection.

Traffic direction is represented by direction of an initial packet which starts the connection.

Action Action which will be taken by *Kerio Personal Firewall* when a connection meeting this rule is detected:

- *Permit* — allows the connection
- *Deny* — blocks the connection

Packet filter rules details

It is important to be aware of how individual parts of a rule and their items are related to be able to define rules effectively.

- The logical relations amog *Protocol*, *Local* and *Remote* are “and”. This implies that only traffic which meets all the conditions will meet the rule.
- The logical relation between items included in one item (protocols, IP addresses and ports) is “or”.

  Example: The *Remote* item consists of two port ranges : 80–88 and 8000–8080. The rule will be met when a remote port belongs to one of these ranges.
- The logical relation between the “IP address” and “port” items in the *Remote* entry is “and”.

Example: The *Remote* entry is specified by the IP address `65.131.55.1` and the port number `80`. This condition will be met by traffic which includes a remote computer with the IP address `65.131.55.1` at the port number `80`.

Notes to Packet Filter Definition

The *Protocol*, *Local* and *Remote* entries are closely related. A user should follow the following rules to ensure smooth functionality of the rule:

1. Port definition is helpful only for TCP and UDP protocols (ports are ignored by other protocols).

   If the rule is available for any protocol (the *Protocol* is not specified), then port numbers are not applicable as they are used only for traffic through TCP or UDP protocols.

2. Application service is specified by port numbers and by protocols. In the packet filter rule dialog, a service is represented by port only — the protocol must be entered by hand.

   Example: Suppose we want to create a rule for incoming HTTP connections (i.e. to enable access to a Web server on a computer which is protected by *Kerio Personal Firewall*), we will take the following steps:

   - *Add port* in the *Local* section. Select the *HTTP* service — this will automatically set the port value to `80`.
   - Go to the *Protocol* section to set TCP, which is used by the HTTP service.

3. The most common traffic model is the client to server communication. The server listens on a predefined port for an incoming connection. A client starts the connection by demanding a free local port (an unknown port) from the operating system that will be used for the connection. This implies that, unlike the server port (which must be always known), any free port can be used temporarily for a client.

   These facts should be considered during packet filter definition. The problem will be better understood through the two following examples:

   Example 1: We intend to enable access to a Web server on a local computer with IP address `60.80.100.120`. We can achieve this by definition of the following rule:

   - *Protocol* — `[6] TCP` (HTTP service uses the TCP protocol)
   - *Local* — `Port: [80] HTTP` (Web server runs on a local computer)

- *Remote* — `Address: 60.80.100.120` (a client represented by a Web browser will be running at a remote host; port is not known yet, that is why we specify the IP address only)

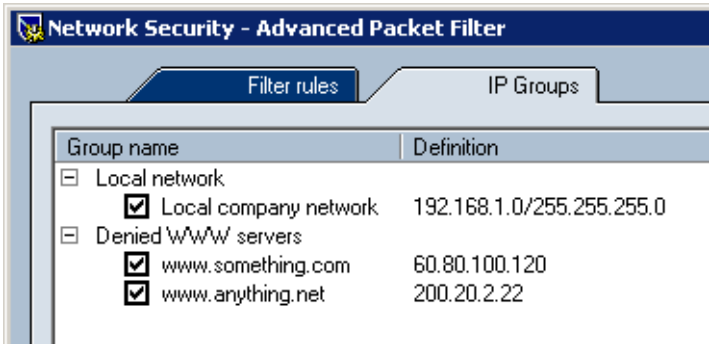
Example 2: We intend to block connections to the Web server with IP address `90.80.70.60`. This is how we define the rule:

- *Protocol* — `[6] TCP`
- *Local* — we leave this entry empty (client port cannot be specified yet)
- *Remote* — `Port: [80] HTTP`, `Address: 90.80.70.60` (specification of the remote server)

IP Groups

IP groups enable easier definition of packet filter rules. These groups can be used for specification of the *Remote* entry in the dialog for packet filter rule definition (see above).

IP groups can be viewed and defined in the *IP Group* tab of the *Advanced Packet Filter* window.

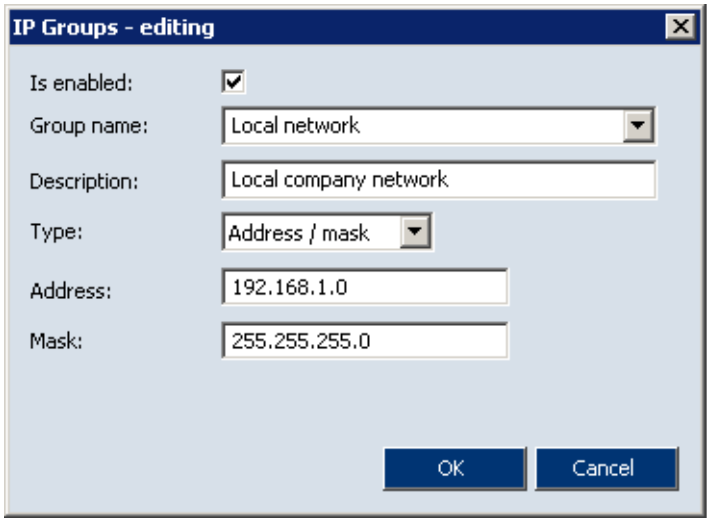


The window consists of the two following columns:

- *Group name* — name of an IP group. Use the plus button to view a list of all items included in a particular group
- *Definition* — definitions of individual items of a particular group

Uncheck an item to disable a rule temporarily. This can be helpful for example when testing or debugging — it is not necessary to remove items and then define them again.

Click on the *Add* button (or the *Edit* button to edit a selected item) to open a dialog for IP group definition.



Is enabled Check/uncheck this option to enable/disable the item. This option is identical to the matching field next to the item name in the *IP Groups* tab (see above). If the *Is enabled* is unchecked, the item is not active. This means that it is not included in the group.

Group name Name of the group to which the item will be included. Specify the item by one of the following methods:

- select a name from the menu — the item will be added to this group
- enter a new group name — this group will be created automatically and the item will be added to the new group

Type Type of the new item:

- *Host* — IP address of one computer
- *Address range* — define *First address* and *Last address* to specify IP range
- *Address / mask* — subnet defined by an IP address and mask
- *Address group* — another IP address group (IP addresses can be embeded into each other)

Chapter 6

System Security

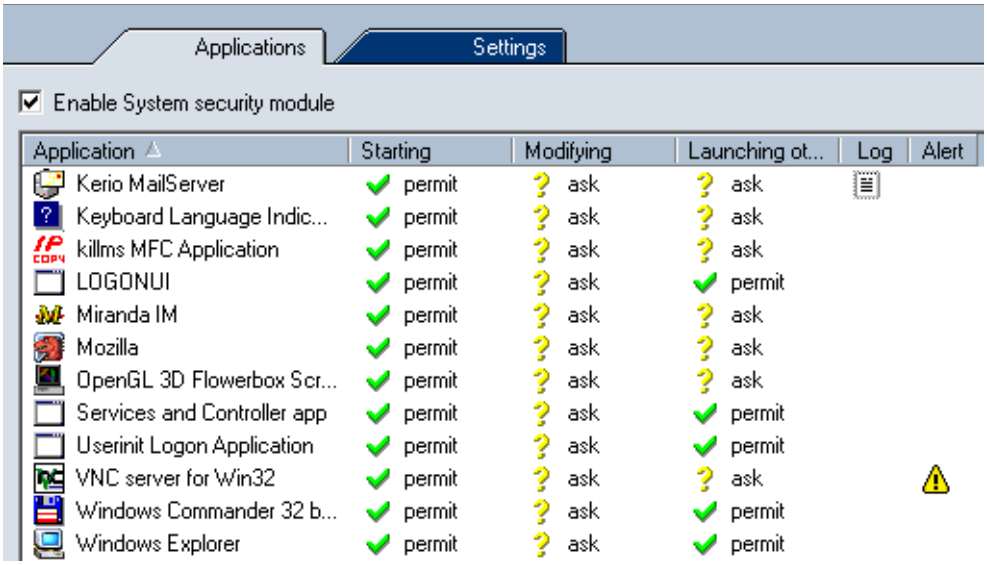
Kerio Personal Firewall controls all applications in the operating system, regardless of whether they are deployed into network communication or not. Therefore it can detect when an application is infected by a new virus or attacked by a Trojan horse immediately (it usually takes some time when an antivirus is used — a new virus must be detected and then an appropriate virus database must be found).

Go to the *System Security* section to set system security parameters (parameters for application control).

Check/uncheck the *Enable System Security module* option to enable/disable control of starting applications. If this option is disabled, running applications is ignored by *Kerio Personal Firewall*.

6.1 Application Rules

Go to the *Applications* tab in the *System Security* section to view and edit rules for startup and change of particular applications.



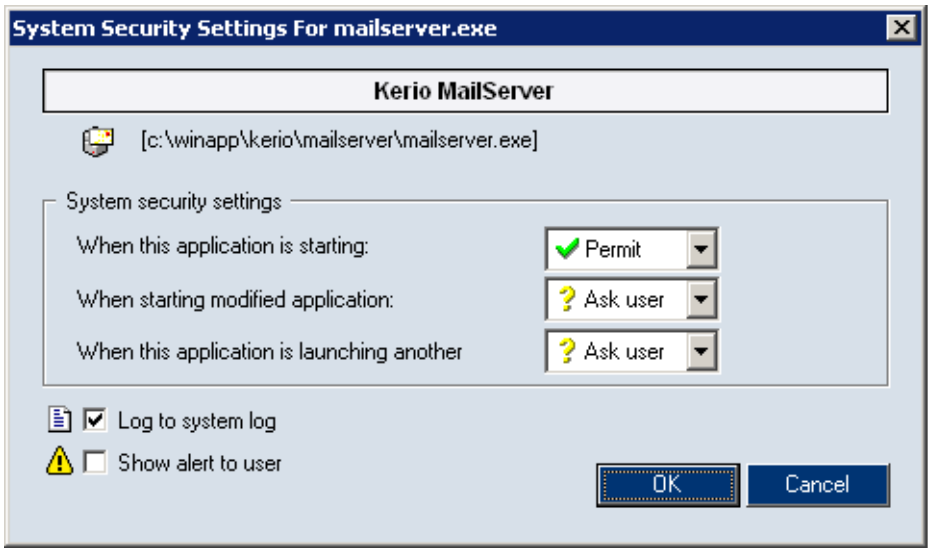
These rules are based on interaction with user when an unknown application is started. Rules cannot be created by hand, they can only be edited or removed.

An action that firewall will take after startup (*Starting*), after the executable file is changed (*Modifying*) and when another application is run by this application (*Launching others*) can be set for each application. Actions can be defined:

1. right from the menu of aplications — click on an action to switch between the following actions: *permit*, *deny* and *ask*

2. right-click on an action and select an action from the context menu

3. in the dialog for rule modification. Use the *Edit* button or the *Edit* option in the context menu to open the dialog.



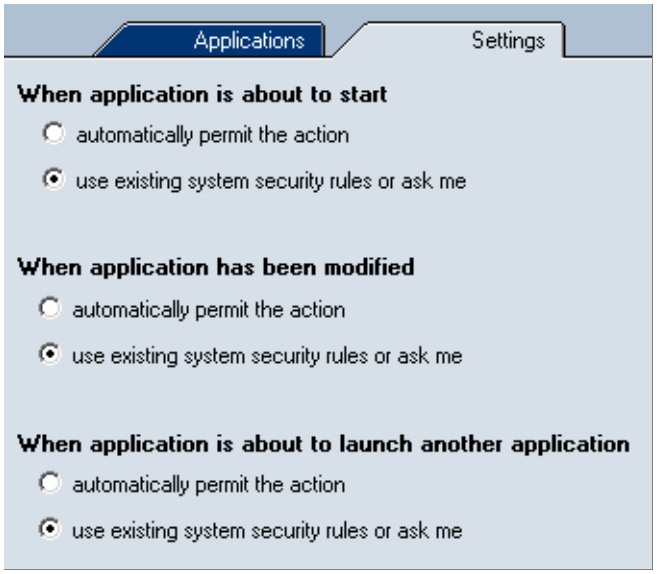
- In the dialog header, description, icon and full path to the application's executable file is provided.

- Use the *System security settings* entry to enable setting actions for the described situations.

- Check or uncheck the *Log to system log* option to enable/disable log activity for the application (startup, change of the executable file or running another application by this application)

- Check or uncheck the *Show alert to user* option to enable/disable the *Alert* dialog (see chapter 3.4) for cases when the application is activated.

6.2 General Rules



Rules in the *Main* tab define how the firewall will behave in the following situations:

- *When application is about to start* — application startup
- *When application has been modified* — modification of application's executable file (by the startup a check-out summary of the executable is performed and it is compared with the summary stored in the *Kerio Personal Firewall* database)
- *When application is about to launch another application* — startup of another application by the running application

One of the following options can be set for each of the situations:

- *automatically permit the action* — *Kerio Personal Firewall* does not block application startup (it accepts change of the executable file)
- *use existing sytem security rules or ask me* — a system security rule for a particular aplication will be used (if it exists) or user will be asked (refer to chapter 3.3)

Chapter 7

Internal Firewall Rules

Kerio Personal Firewall includes predefined rules which allow network communication for exceptional cases (e.g. license registration, product update etc.) and and startup of some applications (system components).

Internal firewall rules are prior to user-defined rules. Internal rules cannot be disabled nor modified.

7.1 Internal Network Traffic Rules

These rules enable allowance of network traffic between individual *Kerio Personal Firewall* components during local or remote administration, connections to *Kerio Technologies* registration or check-for-new-version servers, etc.

Internal network traffic rules are hidden — they are not displayed in *Personal Firewall GUI*.

Remote configuration This rule enables connection of the *Personal Firewall GUI* to the *Personal Firewall Engine*. If remote administration is allowed (see chapter 4.3), connections from any host are allowed. If not, only connection from local host is enabled.

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Rem. adm. enabled	`kpf4ss.exe`	incoming	TCP+UDP	`44334`	any
Rem. adm. disabled	`kpf4ss.exe`	incoming	TCP+UDP	`44334`	`localhost`

Communication between the Personal Firewall GUI and the Engine This rule enables the *Personal Firewall GUI* to connect to the *Personal Firewall Engine* (connection to local or remote administration).

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Unconditional	`kpf4gui.exe`	outgoing	TCP+UDP	`44334`	any

Communication of the Personal Firewall Engine with the GUI This rule allows the *Personal Firewall GUI* to connect to the *Personal Firewall Engine* (displaying of dialogs, notices, warning messages, etc.).

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Rem. adm. enabled	`kpf4ss.exe`	outgoing	TCP+UDP	any	any
Rem. adm. disabled	`kpf4ss.exe`	outgoing	TCP+UDP	any	`localhost`

DNS queries This rule allows *Kerio Personal Firewallu* components to send DNS queries to any DNS server. DNS queries are used for mapping of host names which are later used for various purposes, such as displaying in *Personal Firewall GUI*, resolution of destination IP addresses when accessing a remote administration, etc.

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Unconditional	`kpf4ss.exe`	both	UDP	`53`	any
Unconditional	`kpf4gui.exe`	both	UDP	`53`	any

Sending crashdump files If sending of crashdump files to *Kerio Technologies* (viz kapitola 4.3) is enabled, this rule allows sending files to a corresponding server.

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Sending allowed	`assist.exe`	outgoing	TCP	any	`crashes.kerio.com`

Logging of blocked pop-up and pop-under windows If pop-up blocking is enabled (see chapter 9.1), a special script is used for corresponding webpages that sends *Personal Firewall Engine* information about blocked pages. Traffic is performed by TCP protocol through a special port (`44501`).

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Unconditional	any	outgoing	TCP	`44501`	`localhost`

Update checker This rule allows to access download servers where new versions of *Kerio Personal Firewall* are available.

Note: Server is not specified since various servers can be used for this purpose.

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Proxy server	`kpf4ss.exe`	outgoing	TCP	`proxy_port*`	`proxy_ip*`
Direct access	`kpf4ss.exe`	outgoing	TCP	`80`	any

*) Resolution of IP address and port's proxy server is performed automatically by the *Kerio Personal Firewall* (the information is resolved from configuration of the operating system).

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Proxy server	`kpf4ss.exe`	outgoing	TCP	`prx_port*`	`prx_ip*`
Direct access	`kpf4ss.exe`	outgoing	TCP	`443`	`secure.kerio.com`

Product registration This rule enables registration of *Kerio Personal Firewall* license (see chapter 2.3) on a corresponding server.

*) Resolution of IP address and port's proxy server is performed automatically by the *Kerio Personal Firewall* (the information is resolved from configuration of the operating system).

Syslog If logging to *Syslog* server (refer to chapter 11.3) is enabled, this rule enables connection of the *Personal Firewall Engine* to the *Syslog* server.

Condition	*Aplication*	*Direction*	*Protocol*	*Rem. port*	*Rem. address*
Syslog enabled	`kpf4ss.exe`	outgoing	UDP	`sslg_port*`	`sslg_ip*`

*) IP address and port of the *Syslog* server specified in the *Syslog* section of the *Settings* tab.

7.2 System Security Rules

These rules allow startup of vaqrious components of the operating system on which the *Kerio Personal Firewall* is installed. Internal system security rules can be found in the *System Security / Aplications* section (see chapter 6.1). These rules cannot be removed, however, users can set actions, logging or/and notices for them.

Some of these internal rules are applied only in certain versions of Windows operating systems (some system components differ in individual versions).

Rules for Operating System components

The following symbols are used in the description of system component rules to define file path:

- `WIN_DIR` — the main directory of the Windows operating system (typically, `C:\WINNT` for Windows NT/2000, `C:\WINDOWS` for other versions)
- `SYS_DIR` — system directory of Windows (typically, `C:\WINDOWS\SYSTEM` for Windows 98/Me, `C:\WINNT\SYSTEM32` for Windows NT/2000, and `C:\WINDOWS\SYSTEM32` for Windows XP)

Aplication	*Description*	*Start*	*Modify*	*Launch another*
WIN_DIR\explorer.exe	Windows Explorer	Permit	Ask	Permit

Aplication	*Description*	*Start*	*Modify*	*Launch another*
SYS_DIR\systray.exe	System Tray	Permit	Ask	Permit

1. Rules which are common to all versions of Windows
2. Special rules for Windows 98/ME operating systems
3. Special rules for Windows NT/2000/XP operating systems

Aplication	*Description*	*Start*	*Modify*	*Launch another*
SYS_DIR\services.exe	Services app.	Permit	Ask	Permit
SYS_DIR\winlogon.exe	Logon app.	Permit	Ask	Permit

4. Special rules for Windows 2000/XP operating systems

Aplication	*Description*	*Start*	*Modify*	*Launch another*
SYS_DIR\svchost.exe	Generic Host Proc.	Permit	Ask	Permit

5. Special rules for Windows XP operating system

Aplication	*Description*	*Start*	*Modify*	*Launch another*
SYS_DIR\logonui.exe	Logon UI	Permit	Ask	Permit
SYS_DIR\csrss.exe	Client Server	Permit	Ask	Permit
SYS_DIR\smss.exe	Client Server	Permit	Ask	Permit
SYS_DIR\svchost.exe	Generic Host Proc.	Permit	Ask	Permit

Rules for Kerio Personal Firewall components

These tules allow running individual *Kerio Personal Firewall* applications using special auxiliary programs. The following rules are common to all supported versions of Windows.

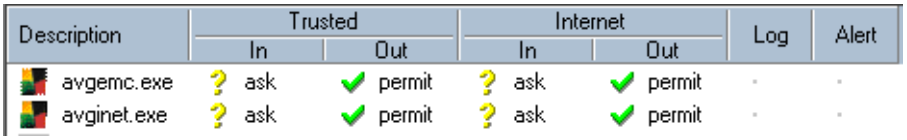
*) The KPF_DIR expression represents a directory (path) where the *Kerio Personal Firewall* is installed

(typically, C:\Program Files\Kerio\Personal Firewall 4).

Aplication	*Description*	*Start*	*Modify*	*Launch another.*
`KPF_DIR\kpf4gui.exe*`	`KPF GUI`	Permit	Permit + log	Permit
`KPF_DIR\kpf4ss.exe*`	`KPF Service`	Permit	Permit + log	Permit
`KPF_DIR\assist.exe*`	`Core dumper`	Permit	Permit + log	Permit
`KPF_DIR\cfgconv.exe*`	`Conf. conv.`	Permit	Permit + log	Permit

7.3 Rules for AVG components

If the *AVG* antivirus is detected when the *Kerio Personal Firewallu* is started first time (immediately after the installation is completed or after the `kpf.cfg` configuration file is removed), the following two rules allowing network traffic for the antivirus components will be added to the *Network security / Applications* section automatically (see chapter 5.2).



- The first rule allows the *AVG E-mail Scanner* component to communicate with mailservers (all data between the mail client and servers will pass through *E-mail Scanner*).
- The second rule allows automatic updates of *AVG* and virus database at corresponding servers.

Rules for *AVG* can be changed and/or removed by a user. If these rules are removed, *Kerio Personal Firewall* will treat communication of *AVG* as an unknown communication.

Warning: If you really use *AVG*, we recommend you not to remove these rules. The removal might block automatic update (the antivirus would not be able to detect new viruses), or problems with email might arise.

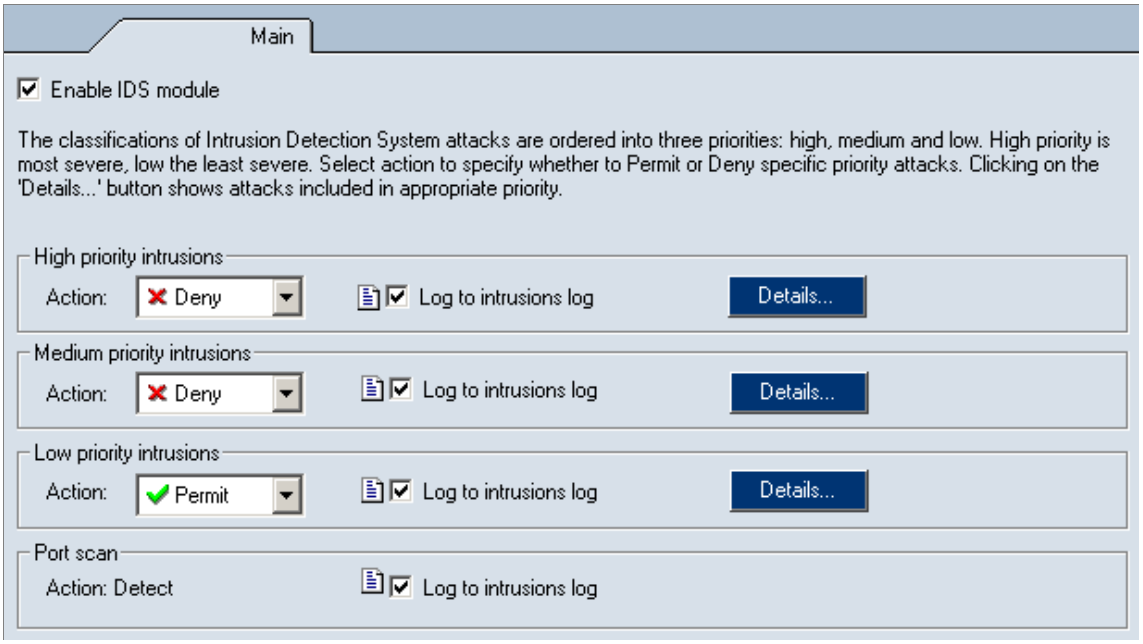
Chapter 8

Intrusions Detection System

Kerio Personal Firewall is able to detect and block many known intrusion types. For this purpose it uses its internal intrusion database. The database is automatically updated every time a new version of the firewall is installed (therefore, we recommend you to perform update of *Kerio Personal Firewall* anytime it is alerted).

8.1 IDS Settings

IDS (Intrusion Detection System) parameters can be set in the *Intrusions* section.



Use the *Enable IDS module* option to enable/disable intrusion detection system.

Kerio Personal Firewall distinguishes between three intrusion types:

- *High priority intrusions* — critical intrusions which might for example damage the operating system, cause data leak, etc.
- *Medium priority intrusions* — intrusions which cause for example blocking of certain services, malfunctions of network connection, etc.

- *Low priority intrusions* — low-level danger intrusions (equivocal network activities, errors in protocols, invalid data format, etc.)

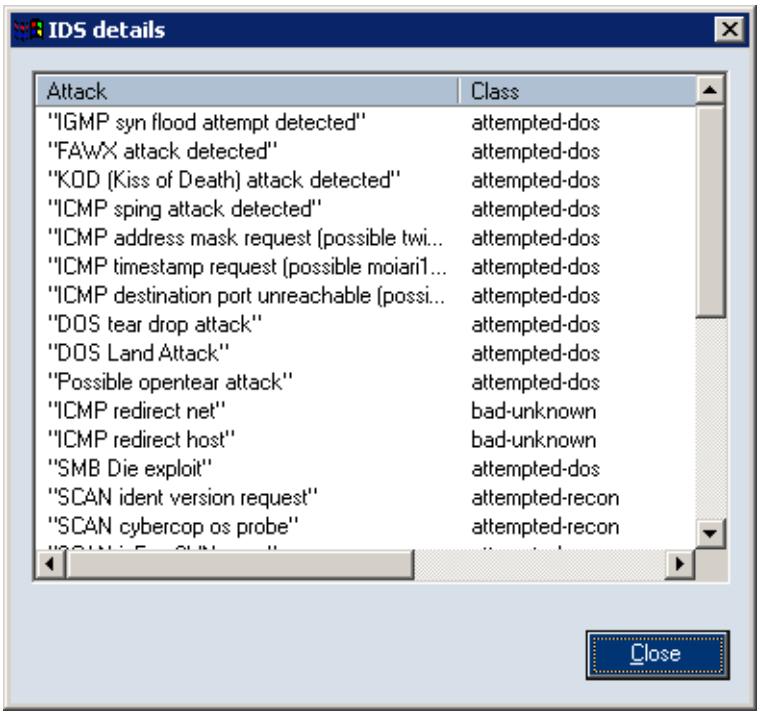
Firewall behaviour can be set for individual types using the following options:

- *Action* — firewall's reactions to attacks of a particular type (*Permit*, *Deny*).

  Generally spoken, it is recommended to deny all *High priority* and *Medium priority* intrusion types — do not permit intrusions of these types unless necessary (i.e. for testing, etc.). *Low priority* intrusions are allowed by default — their blocking might cause malfunctioning of certain services.

- *Log to intrusion log* — logs all detected intrusions of a particular type into the *Intrusions* log (see chapter 8).

Use the *Details* button to open a window providing outline of intrusions of the particular type.



The dialog provides name or description of the attack (the *Attack* column) and class of the intrusion (the *Class* column). *Kerio Personal Firewall* uses the *Snort* IDS — for detailed information on individual attacks and attack types go to the `http:/www.snort.org/` website.

So called *Port Scanning* is a special attack type (detection of open ports on a particular computer). Such attacks cannot be blocked if any ports of the user are open (closed

ports are blocked automatically), they can only be detected. Use the *Log to instrusions log* option to enable/disable logging information on Port Scanning to the *Intrusions* log.

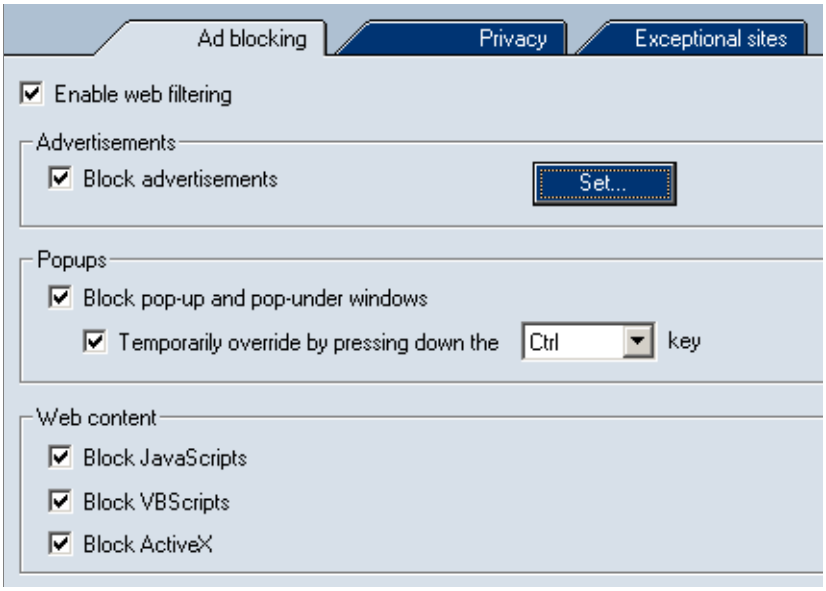
Chapter 9

Web Content Filtering

Two main content filtering functions are available in *Kerio Personal Firewall*:

- Ad blocking (blocking of banners, pop-up windows, etc.)
- Privacy protection (control of outgoing data and stored cookies)

9.1 The *Ad blocking* tab



Kerio Personal Firewall provides the following ad blocking options:

Block advertisement Use this option to block ads according to the defined rules. Use the *Set* button to open a dialog for definiton of these rules (see below).

Block pop-up and pop-under windows Use this option to deny automatic opening of undesirable browser windows (*popup* is a window opened over an active browser window; *pop-under* is a window opened under an active browser window).

Temporarily override by pressing down the ... key If this option is enabled, holding down a selected key (*Ctrl* or *F12*) will temporarily disable pop-up and pop-under windows blocking (i.e. unless a page is loaded).

The *Kerio Personal Firewall* icon on the Systray indicates when pop-up and pop-under blocking is disabled.

Warning: The *F12* key may colide with the *Microsoft* debugger. If you use the *Microsoft Visual Studio*, we recommend you to use the *Ctrl* key.

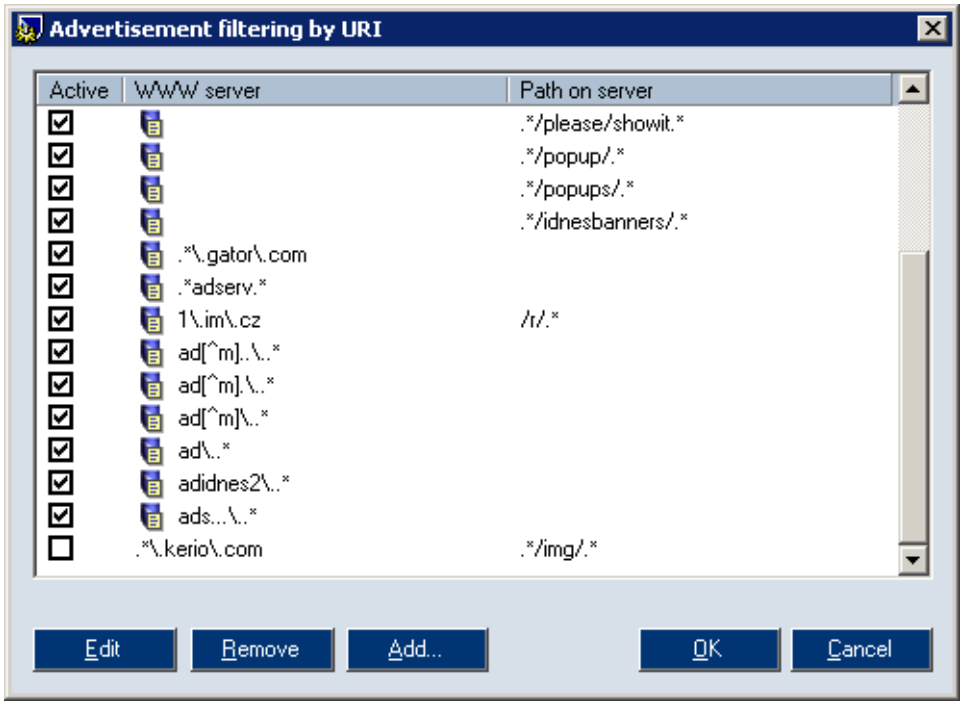
Block JavaScript, Block VBScript Enable these options to filter all commands of the corresponding script run from a website.

Notes: These options might cause problems with displaying of some pages. If so, define special rules for such pages in the *Exception Sites* tab, or disable the *Block pop-up and pop-under windows* option and use another method to filter ads (i.e. the *Block advertisements* option).

These options might cause problems in displaying of some pages or malfunctions — in such cases modify firewall settings as described in the previous item.

Ad Filtering Rules

Click on the *Set* button to open a dialog where ad filtering rules can be edited, removed or added.



Each rule consists of two parts — *Server part* (name or IP address of a particular Web server) and *Local part* (relave address of a particular object at the server).

Only one of these items can be specified.

- If the *WWW Server* item is empty, the rule will be applied on the specified relative address at any server.
- If the *Path on server* entry is empty, the rule will be applied on any object at the specified server (this Web server then cannot be accessed

Use matching fields in the *Active* column to enable/disable individual rules. This way rules can be disabled temporarily (it is not necessary to remove rules and add them later).

Use the *Edit*, *Remove* and *Add* buttons to edit or remove selected rules or to add a new one. *Kerio Personal Firewall* includes set of predefined rules (marked with an icon). Predefined rules cannot be edited nor removed, they can only be enabled or disabled.

Kerio Personal Firewall includes database of predefined rules. These rules are marked with a corresponding icon. Predefined rules cannot be modified or removed, they only can be enabled or disabled. The database is updated whenever a new version of *Kerio Personal Firewall* is installed. Only parameters of the *Active* column will be kept after an update (rules which have been disabled by the user will not be enabled during an update).

Click on the *Add* or the *Edit* button to define ad filtering rules. Such rules consist of two parts:

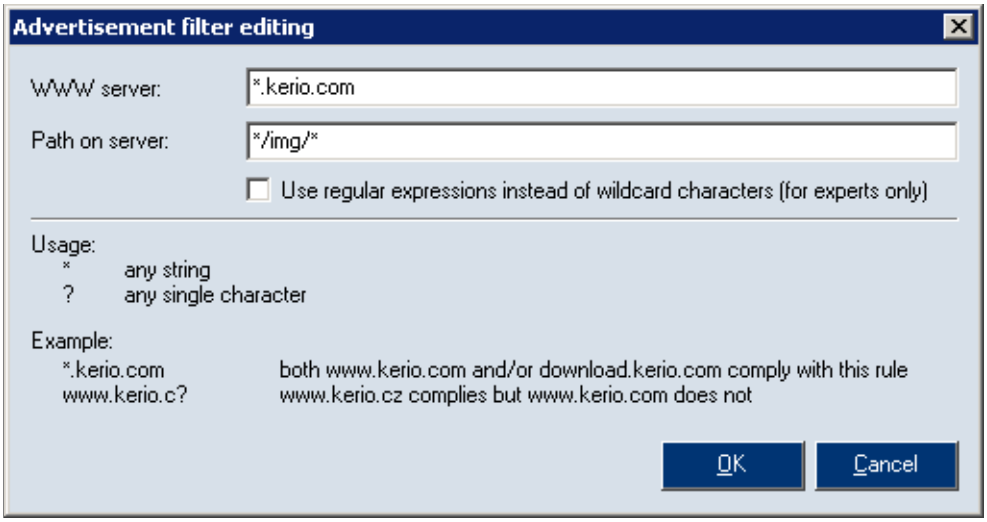
- *WWW server* — name of a WWW server
- Path on server — path to an object (object localization) placed on the server

Both the wildcard characters or the regular expressions (more complex definitions for experienced users) can be used for this definition.

Rule Definition using Wildcard Characters

If the *Use regular expressions instead of wildcard characters* is disabled, the following wildcard characters can be used for definition of the *WWW server* and the *Path on server* entries:

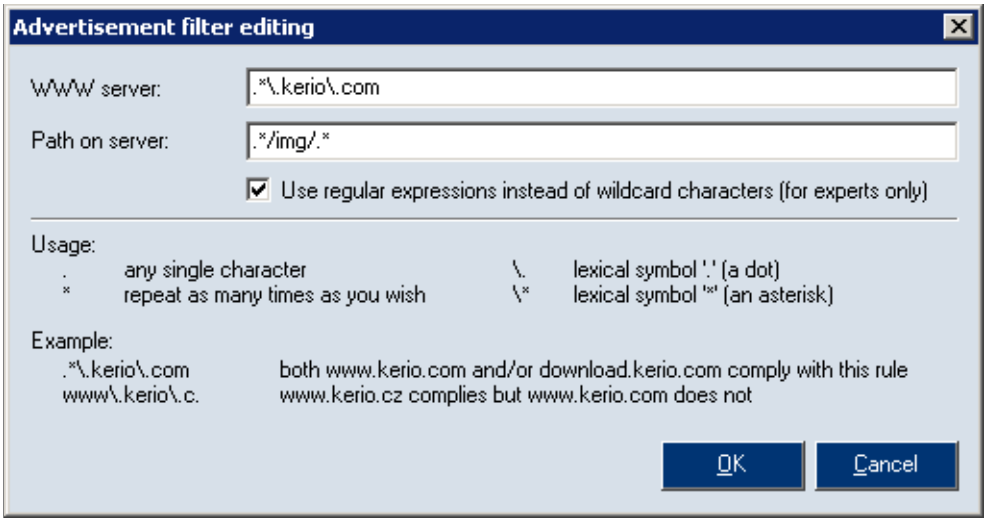
- * (asterisk) — represents any number of characters (even an empty string)
- ? (questionmark) — represents any single character



Examples:

- The *WWW server* entry is defined by the string `*.kerio.com`. Unlike for example `www.akerio.com`, WWW servers `www.kerio.com` or `download.kerio.com` will match with this string.
- The *WWW server* entry contains the string `www.kerio.f?`. WWW servers `www.kerio.fr` nebo `www.kerio.fx` will match with this string, WWW server `www.kerio.com` will not.

Rule Definition using Regular Expressions



If the *Use regular expressions instead of wildcard characters* is enabled, the *WWW server* and the *Path on server* entries must be defined using regular expressions (POSIX standard). Regular expressions can be used to specify any string using special symbols:

A few basic characters are usually sufficient for Web server and Web object definitions:

- `.` (dot) — represents any character in a string.
- * (asterisk) — represents any number (even zero) of repetition of the previous symbol.

  Example: The `.*` expression represents any number of characters.
- \ (backslash) — is used for specification of a character which is used as a special symbol in the regular expression.

  Example: The `\.` expression represents the "dot" character.

Example (refer to the screenshot):

- The *Server Part* item is defined by the `.*ad\.anything\..*` expression.

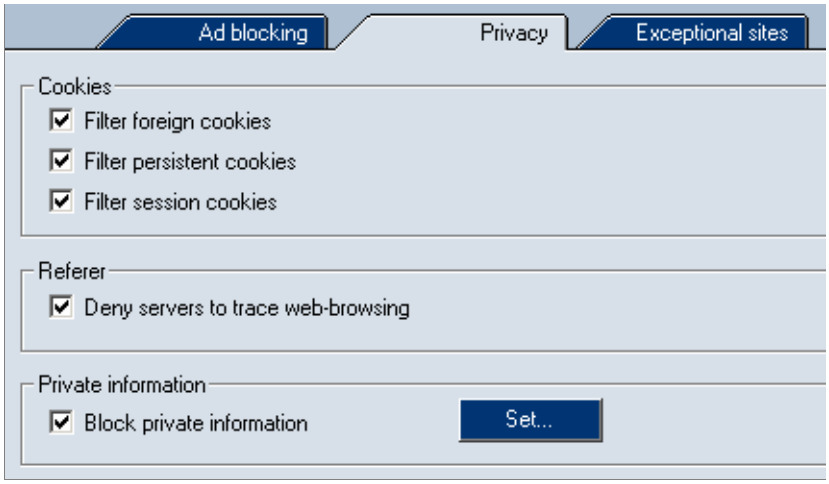
  This expression means that server name must include the `ad.anything.` string — i.e. `ad.anything.net`, `1ad.anything.com`, `img.ad.anything.cx`, etc.
- The *Local Part* s defined by the `.*/img/.*` expression.

  This implies that relative address of the object must include the `/img/` string — i.e. `/img/banner.gif`, `/data/img/bar.jpg` or `/img/`.

For detailed information on regular expressions go to:

`http://www.gnu.org/software/grep/`

9.2 The *Privacy* tab



The *Privacy* tab provides the following options for user privacy protection:

Filter foreign cookies Filtering of both persistent and session cookies from third-party servers (*Third party cookies*).

These cookies are downloaded from servers independent from the page itself (i.e. ad cookies).

Filter persistent cookies This option can be used to filter persistent cookies.

These cookies contain information which can be sent to a particular Web server whenever the page is visited again by the user — the server is informed that the user has already visited the page, this user's preferences and other information.

Filter session cookies This option filters temporary cookies (the cookies are saved during one session only —until the Web browser is closed). These cookies are used only if the user opens a particular page (or a particular server or a server in a particular domain) again within the same session — thay are removed when the all windows of the browser are closed.

Deny servers to trace web-browsing Blocks the `Referer` item in HTTP header.

This item includes URL address of the page from which the user opened the current page. Browsing of users can be easily monitored using the `Referer` item.

Block private information This option blocks sending private user data through forms on Web pages.

Click on the *Set* button to open a dialog where private data which will not be allowed to send and which will be blocked by *Kerio Personal Firewall* can be specified.

Define the following items to specify private user data which will be protected:

- *Type* — information type (i.e. email address, credit card number, etc.).

  This item is for reference only and it is not related to the field type on a Web page.

- *Blocked information* — string which will be blocked by *Kerio Personal Firewall*.

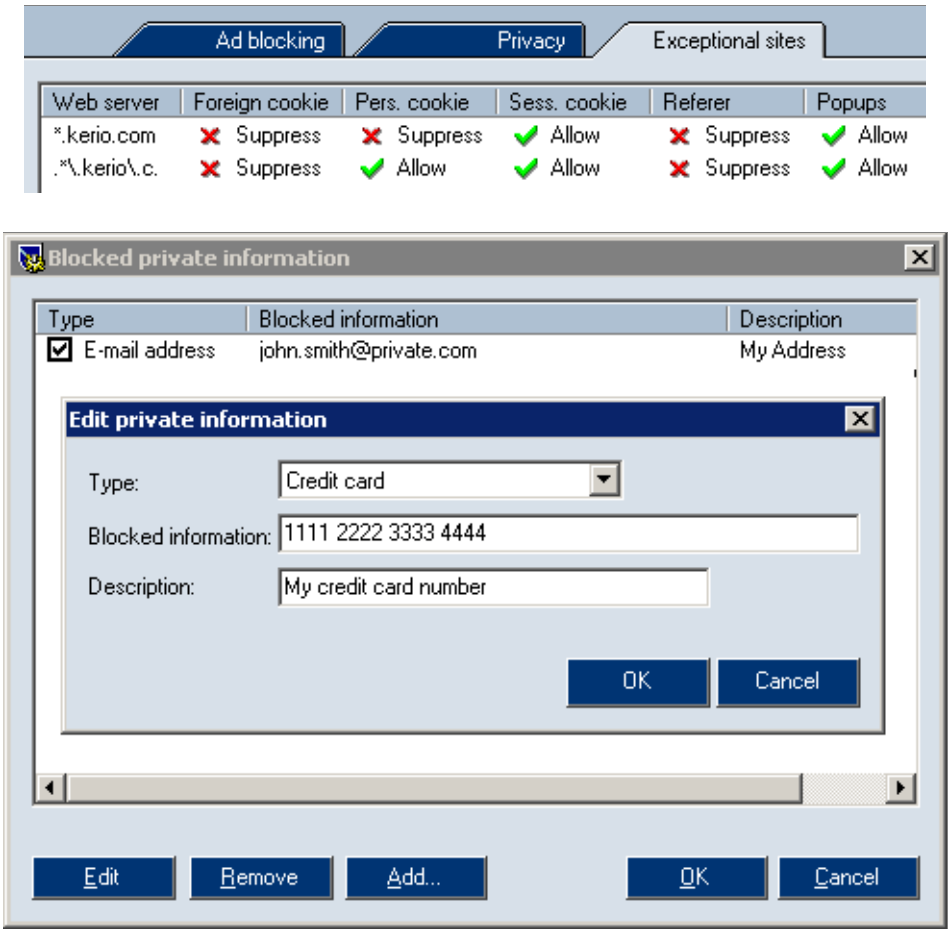
  Warning: Private information is not case-sensitive.

- *Description* — description of the private information (for reference only).

9.3 The *Exceptional sites* tab (exceptions for individual servers)

Web servers for which special Web content filter rules will be defined can be specified in the *Exception sites* tab.

9.3 The *Exceptional sites* tab (exceptions for individual servers)

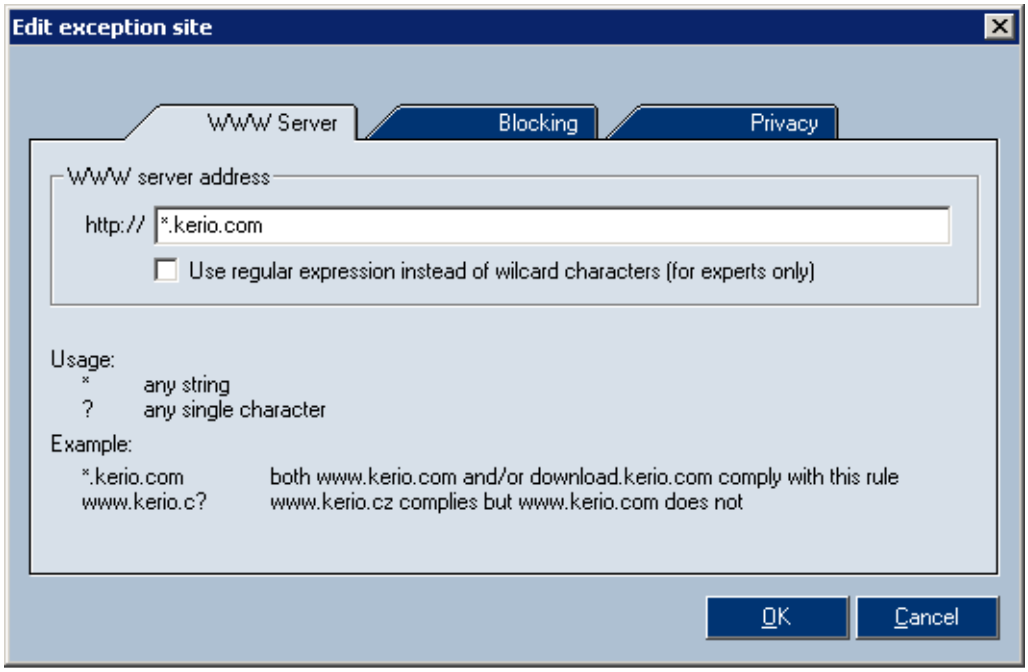


Exceptions for individual Web servers can be helpful especially when general content filter rules (in the *Ad blocking* and *Privacy* tabs) cause that certain Web pages or some of their items do not function (i.e. new windows cannot be opened, it is not possible to login through an email adress, etc.), or that they will be completely blocked (according to ads filtering rules). Before you define an exceptional rules for a server, consider carefully whether the server is trustful or not and which types of objects (scripts, cookies, private data) are really required for smooth functionality of pages on this server.

Use the *Add* or the *Edit* button to open a dialog where exceptions can be defined.

Use the *WWW Server* tab to specify Web server name. Names can be specified by wildcard characters or by regular expressions (see description of the Ad blocking in chapter 9.1).

The *Blocking* and the *Privacy* tabs provide similar functions as the same tabs in the *Web* section. However, in this case individual parameters are applied for a selected Web server only.


Edit exception site
WWW Server
Blocking
Privacy
WWW server address
http://
*.kerio.com
Use regular expression instead of wilcard characters (for experts only)
Usage:
* any string
? any single character
Example:
*.kerio.com both www.kerio.com and/or download.kerio.com comply with this rule
www.kerio.c? www.kerio.cz complies but www.kerio.com does not
OK
Cancel

Chapter 10

Status Information and Logs

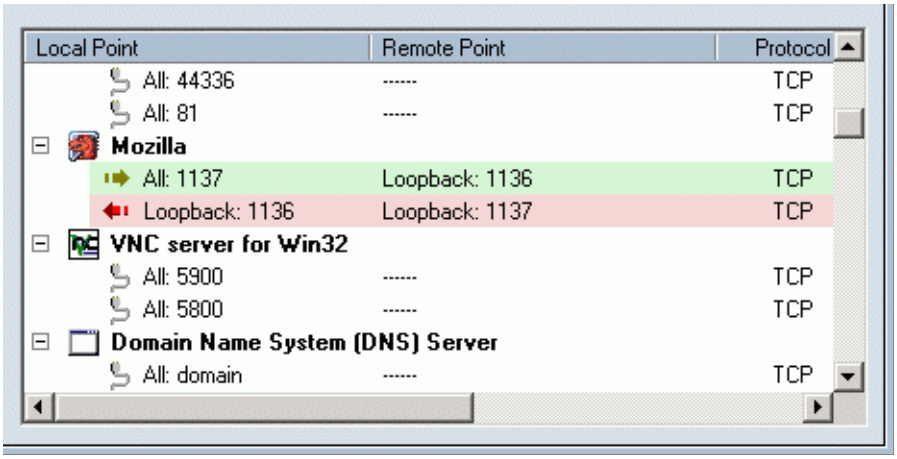
10.1 Connections and Open Ports Overview

Open the *Connections* tab in the *Overview* section to view the list of active connections and open ports used by individual applications. This overview of connections makes users aware of which applications are actively involved in current network communication and which applications are waiting for connections.

A port is considered open when:

- an outgoing connection is established (green background)
- an incoming connection is established (red background)
- an application is listening for connections — server mode (transparent background)

List of applications which include at least one open port can be found in the *Connections* tab.



The first line represents each application's icon and name (description) — if the application has no icon, the default system icon for executable files will be used; if no description (name) is available, the name of the file without the extension will be displayed. Click on the [+] button next to the application icon to view or on the [-] button to hide open ports currently used by the application.

The other lines provide information on individual open connections. Outgoing connections are green, incoming connections are red. Individual columns provide detailed information on each connection:

Local Point Local IP address (or a corresponding DNS name) and port (or name of a service in case of a standard service).

The following special names can be used instead of a DNS name:

- *All* — port is open at all local IP addresses (IP address `0.0.0.0`)
- *Loopback* — local loopback IP address (`127.0.0.1`)

Remote Point IP address (or DNS name) and port number (or a service name) of a particular remote point. The same information for the local IP address and port is provided (see above).

Protocol Used protocol (*TCP*, *UDP*, or both).

Speed In, Speed Out Current speed of incoming (*In*) and outgoing (*Out*) data of the particular connection in kilobytes per second (KB/s).

Bytes In, Bytes Out Total extent of incoming (*In*) and outgoing (*Out*) data within the particular connection.

Note: In case of a port which waits for an incoming connection, only the local IP address, local port and protocol are available.

Summary of Open Ports and Established Connections

Current number of active connections and open ports is displayed at the bottom of the *Connections* tab (in the status line):

- *Connected in* — number of established incoming connections
- *Connected out* — number of established outgoing connections
- *Listening* — number of ports at which application wait for connection

10.2 Statistics

In the *Overview / Statistics* section you can view system statistics for intrusion detection and Web content filter.

Use the *Show statistics for the last ...* entry to view statistics for a selected time range:

- *hour* — last hour
- *day* — last day
- *week* — last week
- *month* — last month

The *Reset all statistics* button can be used to reset all monitored statistics. This action must be confirmed by the user.

Statistics are divided into the following groups according to their types. Click on a group name to view corresponding statistics (*WWW* or *Intrusions* — for details refer to chapters 11.7 and 11.6).

Advertisements Blocked ads and web pages components:

- *Advertisements* — number of objects blocked by ad filtering rules
- *Popups* — number of blocked pop-up and pop-under windows

Scripts

- *JavaScripts* — number of filtered *JavaScript* items
- *VBScripts* — number of filtered *Visual Basic Script* items
- *ActiveX* — number of filtered ActiveX components

Intrusions Number of detected intrusions:

- *High* — critical intrusions
- *Medium* — medium priority intrusions (i.e. service blocking)
- *Low* — low priority intrusions (i.e. queer activities)
- *Port scans* — the *Port Scanning* function

Privacy Number of objects blocked by the Privacy function:

- *Referers* —number of `Referer` items filtered from the HTTP header
- *Private information* — number of blocked private items that were to be sent

Cookies Number of iltered cookies of the following types:

- *Persistent cookies* — number of filtered cookies
- *Session cookies* — number of filtered temporary cookies
- *Foreign cookies* — number of filtered third party cookies

Chapter 11

Logs

Logs are files where history of certain items is stored.

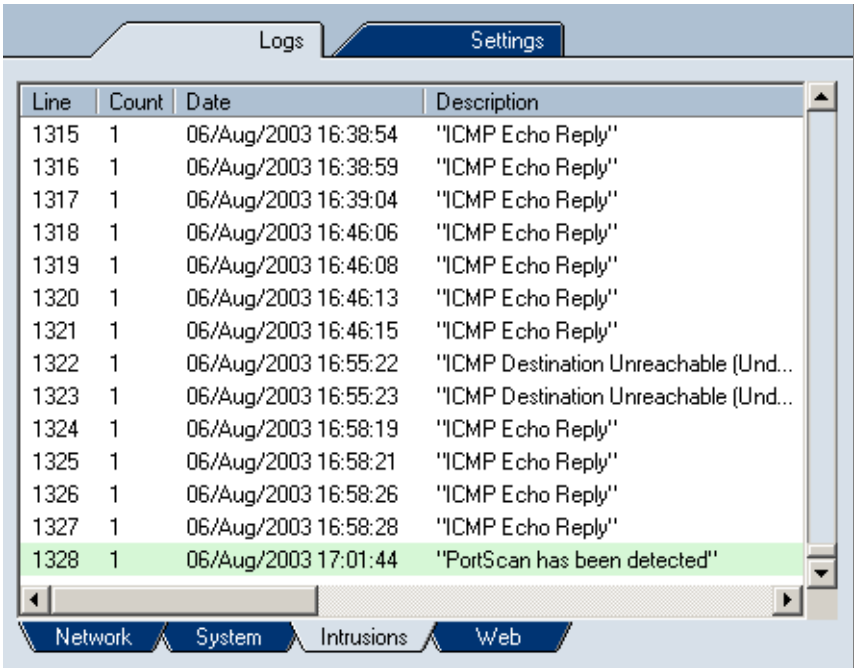
Kerio Personal Firewall provides a log for each module (*Network*, *System*, *Intrusions* and *Web*).

The other logs (*Error*, *Warning* and *Debug*) store information on processes of *Kerio Personal Firewall*. This information can for example help the *Kerio Technologies* technical support to solve your possible problems with the firewall.

Log files are stored in the `logs` subdirectory of the directory where *Kerio Personal Firewall* is installed (typically `C:\Program Files\Kerio\Personal Firewall 4\logs`). The file has the `.log` extension (i.e. `network.log`). An index file (for scanning) is included in each log. This file has the `.idx` extension (i.e. `network.log.idx`).

11.1 Logs Viewing

Individual firewall module logs can be viewed and logging parameters can be set in the *Logs & Alerts* section.



The *Logs* section includes tabs with logs for individual firewall modules. Each tab is focused on a certain part of a particular log file. Click on a column name to reorder the log items.

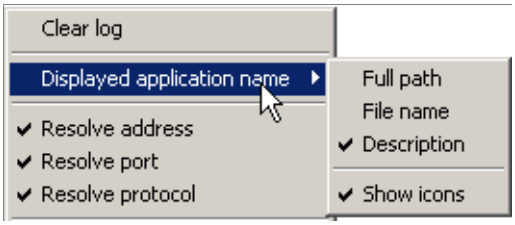
For technical reasons (data size), log files are not downloaded to the disc complete. Only the part which are to be viewed is downloaded. Therefore, the following difficulties may occur:

- Logs display slowly.
- In ordering by columns only currently viewed part of the log is displayed. Information must be ordered again after another part of the log is viewed.

Note: The *Error*, *Warning* and *Debug* logs are not available from the *Kerio Personal Firewall* user interface — they can be viewed only as files.

11.2 Logs Context Menu

Right-click on the log tab to open a context menu providing options for a particular log:



Clear log Clears the log. ll data will be removed from a corresponding file. Removed files cannot be refreshed.

Displayed application name The way how application names will be displayed:

- *Full path* — full path to the application's executable file
- *File name* — name of the application's executable
- *Description* — description of the application (if it is not available, name of the executable without the extension is displayed)

Check/ uncheck the *Show icons* option to enable/disable showing icons (the system icon for executables will be used if the application has no icon).

Resolve address Names of computers will be displayed instead of IP addresses.

Computer names are found through DNS. Unless a name is found, IP address will be displayed.

Resolve port Names of services willbe displayed instead of port numbers (this function is available only for standard services defined in the `services` system file).

Resolve protocol Names of protocols will be displayed instead of protocol numbers (this function is available only for standard protocols defined in the `protocols` system file).

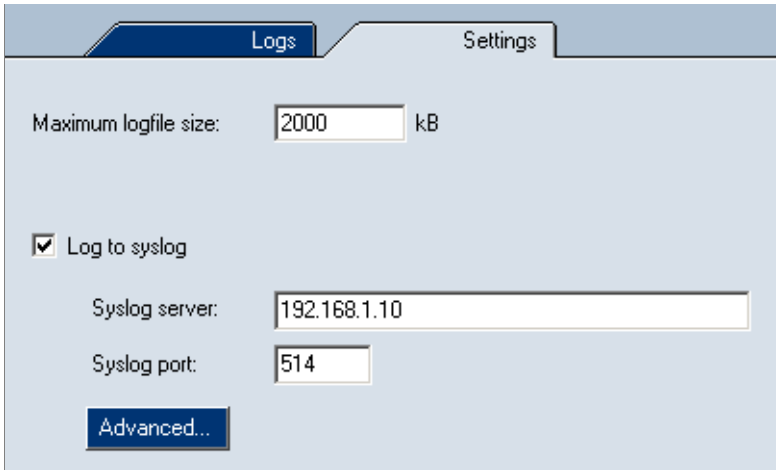
Note:

1. Some logs do not provide all items mentioned above — i.e. no network communication is displayed for the *System* log. Therefore *Resolve address*, *Resolve port* and *Resolve protocol* functions are not available.

2. The *Displayed application name* and *Resolve address/port/protocol* options are applied globally — their setting influences all logs, the *Overview / Connections* section (see chapter 10.1), *Connection alert* (see chapter 3.2) and *Starting / Replacing application* dialogs (see chapter 3.3) and the *Alert* window (refer to chapter 3.4). View configuration is also described in corresponding chapters.

11.3 Log Options

The following parameters and log options (applied generally on all *Kerio Personal Firewall* logs) can be set in the *Settings* tab of the *Logs & Alerts* section:

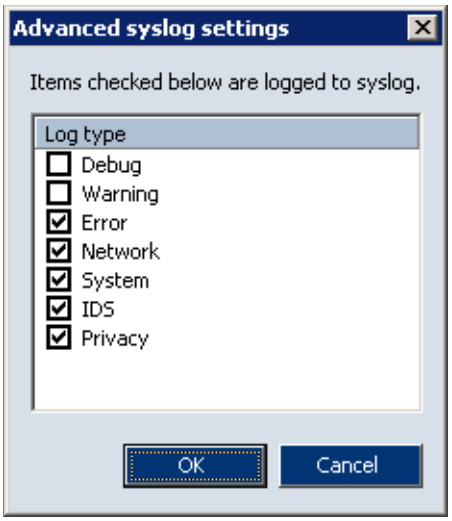


Maximum log file size Maximal size of a log file (in kilobytes). If the size is exceede, the file will be removed and a new log will be started.

Log to Syslog Check/uncheck this option to enable/disablesending selected files to *Syslog* server.

Specify *Syslog server* through name and IP address of the corresponding *Syslog* server and define the *Syslog port* entry with number of the port on which the *Syslog* server is running (514 by default).

Click on the *Advanced...* button to open a dialog for selection of *Kerio Personal Firewall* logs which will be sent to the *Syslog* server.



11.4 Network Log

Information on network traffic which is meeting an application rule (see chapter 5.2) or a packet filter rule (refer to chapter 5.5). Traffic is not logged unless the *Log communication to network log* option is enabled.

The *Network* log provides the following information:

Line	Count	Date	Application	Direction	Local...	Remote point	Protoc
0	1	06/Aug/2003 16:55:10	Mozilla	out	ferda...	128.242.10...	TCP
1	1	06/Aug/2003 16:55:12	Mozilla	out	ferda...	128.242.10...	TCP

- *Line* — log line number
- *Count* — number of records (if one record is repeated in sequence, it is logged only once and the real count is expressed by a numeral)
- *Date* — date and time when the event was logged

- *Description* — description of a particular packet filter rule
- *Application* — name of a local application (according to the *Displayed application name* parameter) participating in the particular network communication

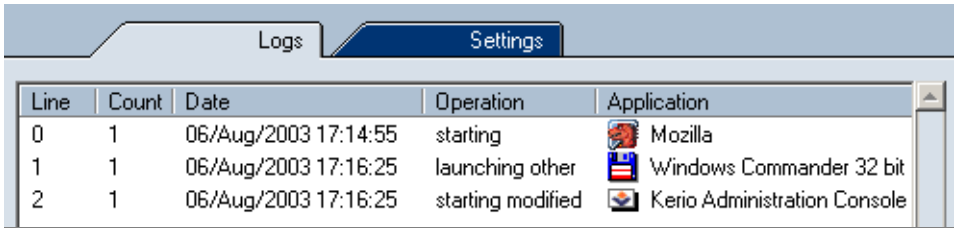
  Note: Both description of applications and full paths to their executable files are saved into the log file. Therefore, you can switch between the two items and select which one will be displayed.
- *Direction* — direction of the connection (*in* — to a local computer, *out* — from a local computer)
- *Local point* — local IP address (name of the computer)
- *Remote point* — IP address (name) of the remote computer
- *Protocol* — used communication protocol (TCP, UDP, etc.)
- *Action* — action which was taken:
  - *permitted* — the communication has been permitted
  - *denied* — the traffic has been denied
  - *asked → permitted* — user was asked through the *Connection alert* dialog and the communication has been permitted
  - *asked → denied* — user was asked through the *Connection alert* dialog and the communication has been denied

11.5 System Log

Information on running applications which meet corresponding rules in the

System Security / Applications section is stored in the *System* log. The *Log to system log* option must be enabled for a particular rule to enable the log.

The *System* log provides the following information:

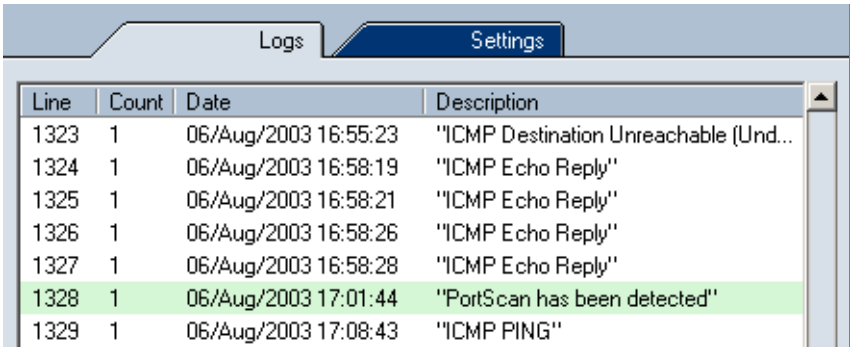


- *Line* — log line number
- *Count* — number of identical records
- *Date* — date and time when the event was logged
- *Operation* — operation type:
  - *starting* — the application is starting
  - *starting modified* — executable file of the application has been changed
  - *launching other* — the application is launching another application
- *Application* — application name (with respect to the *Displayed application name* parameter)
- *Subject* — this item represents name of an application started by the original application (with respect to the *Displayed application name* parameter)
- *Action* — action which was taken:
  - *permitted* — running the application has been permitted
  - *denied* — running the application has been denied
  - *asked* → *permitted* — user was asked through the *Starting/Replacing application* dialog and start of the application has been permitted
  - *asked* → *denied* — user was asked through the *Starting/Replacing/Launching other application* dialog and start of the application has been denied

11.6 Intrusions Log

Information on detected intrusions is logged into the *Intrusions* log. Only intrusions belonging to the types where the *Log to intrusions log* option is enabled are logged (see chapter 8).

The *Intrusions* log provides the following information:

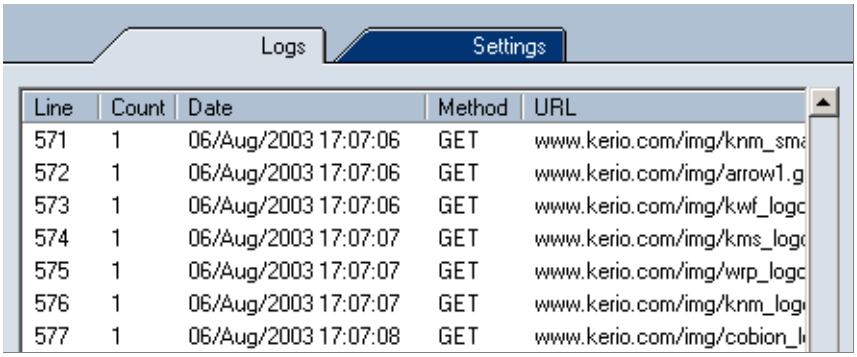


- *Line* — log line number
- *Count* — number of identical records
- *Date* — date and time when the event was logged
- *Description* — name (description) of detected intrusion (refer to chapter 8)
- *Direction* — direction of the intrusion (intrusions might be also initiated from local computers)
- *Remote address* — IP address (name) of the remote computer (if detectable— intrusions may be initiated from false IP addresses)
- *Reference URL* — URL pages to which users can refer to read detailed information on ap articular intrusion (if available)

11.7 Web Log

Information on objects blocked by the Web content filter is logged into the *Web* log. This log is not configurable — if the Web content filter is enabled (see chapter 9), all filtered objects are logged.

The *Web* log provides the following information:



- *Line* — log line number
- *Count* — number of identical records
- *Date* — date and time when the event was logged
- *Method* — used method of the HTTP protocol (*GET* or *POST*)
- *URL* — URL address of the object (of the page) to which the method is applied
- *Subject* — type of the blocked item of a Web page (*referer*, *cookie*, *blockPopups* — pop-up or pop-under windows)
- *Value* — value of this item (content of the `Referer:` item, information in cookie or rule which was used to block the ad)
- *Action* — action which was taken (*Removed* — the item was removed from the Web page, *Blocked* — the item was blocked by ad rules)

Information provided within the *Value* item depends on a type of the blocked object (see the *Subject* item):

- *Advertisement* — the *Value* column provides information on a rule which has been applied (see chapter 9.1)
- the `Referer` item — the *Value* column provides URL address of the page which the item referred to
- *Script* — type of the filtered object is provided in the *Value* column (*JavaScript*, *VBScript* or *ActiveX*).
- *blockPopups* — the *ON* expression in the *Value* column informs users that pop-up and pop-under windows blocking is enabled for the particular page.

11.8 Debug, Error, Warning Logs

Debug Log

The *Debug* log includes detailed information on all processes of *Kerio Personal Firewall*.

Error Log

Errors which seriously affect functionality of *Kerio Personal Firewall* (i.e. the *Personal Firewall Engine* cannot be started) are logged into the *Error* log.

Warning Log

Less important errors are logged into the *Warning* log (i.e. an error detected when a check for new version is performed, etc.).

Chapter 12

Glossary

Application protocol Application protocols are transmitted in packets of TCP or UDP protocol. They are used for transmission of user (application) data. In addition to standard application protocols which are available (i.e. SMTP, POP3, HTTP, FTP, etc.), application programmers may use a custom (non-standard) method for communication.

Cookie Information in text format that the server stores at a client (Web browser). It is used for later identification of a user when the same server/site is opened again. Cookies can be misused for monitoring which sites have been visited by a user, or they can be used for visit counter.

Firewall A tool (usually a software product) for protection from intrusions and from data outflow. Two basic firewall types are available:

- network firewall — protects computers of a network. Usually, it is used as a gateway (router) through which the particular network is connected to the Internet.
- personal firewall — protects one computer (user's workstation). Unlike network firewalls, it can match network communication with a particular application, change its behavior accordingly to interaction with users, etc.

Note: In this guide the word *firewall* represents *Kerio Personal Firewall*.

ICMP *ICMP* (Internet Control Message Protocol) is a protocol used for transmission of control messages. Several types of such messages are available, such as a report that the destination is not available, redirection request or response request (used in the *PING* command).

IP *IP* (Internet Protocol) is a protocol transmitting all Internet protocols in its data part. The header of this protocol provides essential routing information, such as source and destination IP address (which computer sent the message and to which computer the message should be delivered).

Port The most essential information in TCP and UDP packet is the source and destination port. The IP address identifies a computer in the Internet, whereas a port identifies an application running on the computer. Ports 1–1023 are reserved for

standard services and the operating system, whereas ports 1024–65535 can be used by any application. In a typical client to server connection, usually the destination port is known (connection is established for this port or UDP datagram is sent to it). The source port is then assigned by the operating system automatically.

TCP *TCP* (Transmission Control Protocol) is used for reliable data transmission through so called virtual channel (connection). It is used as a transmission protocol for most application protocols, such as SMTP, POP3, HTTP, FTP, Telnet, etc.

TCP/IP *TCP/IP* is a general term for protocols used in communication over the Internet. Data is divided into data items called packets within individual protocols. Each packet consists of a header and a data part. The header includes routing information (i.e. source and destination address) and the data part contains transmitted data.

The Internet protocol stack is divided into several levels. Packets of lower protocols encapsulate parts of higher-level protocols in their data parts (i.e. packets of TCP protocol are transmitted in IP packets).

UDP *UDP* (User Datagram Protocol) is a so called connectionless protocol. This implies that it does not create any connection and data is transmitted in individual messages (so called datagrams). UDP does not warrant reliable data delivery (datagrams can be lost during transmission). However, unlike transmission through TCP protocol, it provides faster data transmission (it is not necessary to establish connections or provide reliability control, confirmation is not demanded, etc.). UDP protocol is used especially for transmission of DNS queries, audio files, video files, or other types of streaming media which promote speed over reliability.